

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-134126

(43)Date of publication of application : 22.05.1998

(51)Int.Cl. G06F 19/00
 G06K 17/00
 G07D 9/00
 G07D 9/00
 G07F 19/00

(21)Application number : 08-291531

(71)Applicant : N T T DATA TSUSHIN KK

(22)Date of filing : 01.11.1996

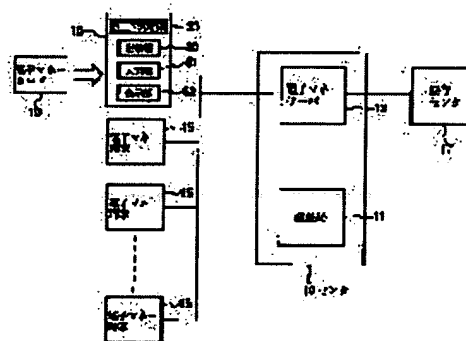
(72)Inventor : FURUHASHI NOBUO
 HETA SATOSHI
 SHIBATA ATSUSHI
 SHINKAI ICHIRO
 KITADA TOYOHIRO

(54) ELECTRONIC MONEY SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent money data from being forged and to easily detect an illegal transaction by transferring transaction money instructed with a transfer instruction message from a center from a specific account to the account specified with the transfer instruction message and sending a transfer completion message to the center after the transfer is completed.

SOLUTION: A bank center 17 has a settlement account as the account of a user (bearer) of an electronic money card 19 and a special account as the operation account of electronic money that the bank has, and perform money reception and payment between those accounts. Namely, the bank center 17 once receiving a money payment message from an electronic money server 13 decides the account number corresponding to the card ID by referring to an account table. Then the balance of the settlement account of this account number is checked and when it is decided that the balance is larger than an indicated amount of money, it is decided that the money can be paid, thereby moving (transferring) the specific money from the settlement account to the special account. Then a money payment completion message reporting the transfer completion is sent to the electronic money server 13.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-134126

(43)公開日 平成10年(1998) 5月22日

(51)Int.Cl.⁹

識別記号

F I

G 0 6 F 19/00

G 0 6 F 15/30

3 5 0 A

G 0 6 K 17/00

G 0 6 K 17/00

L

G 0 7 D 9/00

4 3 1

G 0 7 D 9/00

4 3 1 Z

4 3 6

4 3 6 Z

G 0 7 F 19/00

4 7 6

審査請求 未請求 請求項の数18 O L (全 31 頁)

(21)出願番号

特願平8-291531

(22)出願日

平成8年(1996)11月1日

(71)出願人 000102728

エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目3番3号

(72)発明者 古橋 信夫

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72)発明者 部田 智

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72)発明者 柴田 淳

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(74)代理人 弁理士 木村 満

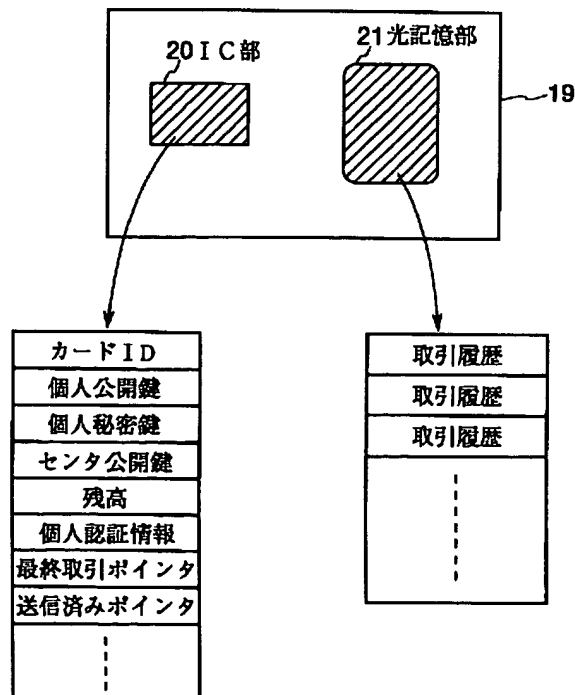
最終頁に続く

(54)【発明の名称】 電子マネーシステム

(57)【要約】

【課題】 金銭データの偽造等を有効に防止し、且つ、不正な取引を容易に検出することを可能とする電子マネーシステムを提供することを目的とする。

【解決手段】 金銭的価値を有する電子マネーを格納する電子マネーカード19を用いて電子マネーを取引する電子マネーシステムにおいて、電子マネーカード19として、IC部20と光記憶部21とを備えるものを使用する。IC部20には、電子マネーカード19を特定するための情報、残高、光記憶部21をアクセスするための情報等を記録し、光記憶部21には、その電子マネーカードを用いて行われた電子マネーの取引の全ての履歴を記録する。電子マネー取引システムのコンピュータにも取引履歴を登録する。取引履歴を追跡することにより、不正の発生箇所、金額等を検出できる。



【特許請求の範囲】

【請求項1】追記型記憶部とICメモリ部とを備え、金銭的価値に関する情報を格納する電子マネーカードと、前記電子マネーカードを処理する端末と、前記端末と通信回線で接続され、前記端末を制御するセンタと、前記センタに通信回線で接続された銀行コンピュータと、より構成される電子マネーシステムであって、前記電子マネーカードの前記追記型記憶部は取引履歴情報を記憶し、

前記電子マネーカードの前記ICメモリ部は、前記追記型記憶部に記憶された取引履歴情報の位置を示す位置情報を記憶し、

前記端末は、換金を含む電子マネーの取引の指示と取引金額を入力するための入力手段と、前記入力手段により入力された前記取引の指示のうちの換金指示と取引金額に基づいた換金依頼電文を前記センタに送信する換金依頼送信手段と、前記センタからの換金終了電文に回答し、前記電子マネーカードの前記ICメモリ部に格納された前記位置情報に従って、該換金処理に関する取引履歴情報を前記電子マネーカードの前記追記型記憶部に書き込む手段と、を備え、

前記センタは、前記端末からの前記換金依頼電文を受信し、受信した該換金依頼電文に基づいた振替指示電文を前記銀行コンピュータに送信する手段と、前記銀行コンピュータからの振替完了電文に回答して、前記端末に前記換金終了電文を送信する手段と、を備え、

前記銀行コンピュータは、前記センタからの前記振替指示電文により指示された取引金額を所定口座から該振替指示電文により特定された口座に振り替える振替手段と、前記振替手段による振替が完了すると前記振替完了電文を前記センタに送信する手段と、を備え、ことを特徴とする電子マネーシステム。

【請求項2】前記電子マネーカードの前記追記型記憶部と前記ICメモリ部の少なくとも一方は、口座を特定するための口座特定情報を記憶し、

前記換金依頼送信手段は、前記電子マネーカードに記憶された前記口座特定情報を読み出し、前記換金依頼電文に含ませる手段を更に備える、

ことを特徴とする請求項1に記載の電子マネーシステム。

【請求項3】前記端末は、前記電子マネーカードが保有している残高が前記入力手段により入力された前記取引金額以上か否かを判別し、前記残高が前記取引金額未満ならば、エラーメッセージを表示すると共に取引を中止若しくは金額の再入力を要求する手段を備える、ことを特徴とする請求項1、又は2に記載の電子マネーシステム。

【請求項4】前記センタは、前記電子マネーカードの残高を記憶する残高記憶手段と、前記電子マネーカードから受信した前記換金依頼電文により指示された取引金額

を前記残高記憶手段に記憶されている該電子マネーカードの残高より差し引く残高更新手段と、を備える、ことを特徴とする請求項1乃至3のいずれか1項に記載の電子マネーシステム。

【請求項5】前記センタは、前記電子マネーカードから受信した前記換金依頼電文により指示された取引金額が前記残高記憶手段に記憶されている該電子マネーカードの残高以下か否かを判別し、前記残高が前記取引金額未満ならば、取引の中止若しくは金額の再入力を指示する指示電文を前記端末に送信する手段と、を備える、ことを特徴とする請求項4に記載の電子マネーシステム。

【請求項6】前記取引履歴情報は、各取引について、取引の種別と、取引年月日と、その取引を処理した前記端末を特定する情報と、取引金額とを含む、ことを特徴とする請求項1乃至5のいずれか1項に記載の電子マネーシステム。

【請求項7】前記電子マネーカードの前記追記型記憶部は、該電子マネーカードで取引された全ての取引の取引履歴を記憶する、ことを特徴とする請求項1乃至6のいずれか1項に記載の電子マネーシステム。

【請求項8】前記センタは、前記電子マネーカードで取引された全ての取引の取引履歴を記憶する取引履歴記憶手段を備える、ことを特徴とする請求項1乃至7のいずれか1項に記載の電子マネーシステム。

【請求項9】前記電子マネーカードの前記追記型記憶部と前記ICメモリ部との少なくとも一方はその電子マネーカードのカード識別符号を記憶し、

前記換金依頼電文は、前記電子マネーカードの前記カード識別符号を含み、

前記センタは、使用を認めない前記電子マネーカードの前記カード識別符号を不正カードIDとして記憶する不正カードID記憶手段と、前記換金依頼電文に含まれる前記カード識別符号と前記不正カードID記憶手段に記憶されている前記不正カードIDとを比較し、一致する不正カードIDを検出すると、取引を中止する手段を備える、ことを特徴とする請求項1乃至8のいずれか1項に記載の電子マネーシステム。

【請求項10】前記端末は、端末識別符号を記憶し、前記換金依頼電文は、前記端末識別符号を含み、前記センタは、使用を認めない前記端末の前記端末識別符号を不正端末IDとして記憶する不正端末ID記憶手段と、前記換金依頼電文に含まれる前記端末識別符号を前記不正端末ID記憶手段に記憶される前記不正端末IDと比較し、一致する不正端末IDを検出すると、取引を中止する手段を備える、ことを特徴とする請求項1乃至9のいずれか1項に記載の電子マネーシステム。

【請求項11】前記電子マネーカードの個人公開鍵を記憶する個人情報記憶手段を備える認証局を更に備え、前記電子マネーカードの前記ICメモリ部は前記個人公開鍵を記憶し、

3

前記換金依頼電文は、前記電子マネーカードの前記個人公開鍵を含み、

前記センタは、受信した前記換金依頼電文のうち、前記個人公開鍵を前記認証局に送信する個人鍵送信手段を備え、

前記認証局は、受信した前記個人公開鍵が前記個人情報記憶手段に記憶されている前記個人公開鍵のいずれかと一致するか否かを判別し、一致しない場合、取引不可の旨のメッセージを前記端末に送信し、取引を中止する手段を更に備える、

ことを特徴とする請求項1乃至10のいずれか1項に記載の電子マネーシステム。

【請求項12】前記電子マネーカードのカード識別符号を記憶する個人情報記憶手段を備える認証局を更に備え、

前記電子マネーカードの前記ICメモリ部は前記カード識別符号を記憶し、

前記換金依頼電文は、前記電子マネーカードの前記カード識別符号を含み、

前記センタは、受信した前記換金依頼電文のうち、前記カード識別符号を前記認証局に送信する手段を備え、

前記認証局は、受信した前記カード識別符号が前記個人情報記憶手段に記憶されている前記カード識別符号のいずれかと一致するか否かを判別し、一致しない場合、取引不可の旨のメッセージを前記端末に送信し、取引を中止する手段を更に備える、

ことを特徴とする請求項1乃至11のいずれか1項に記載の電子マネーシステム。

【請求項13】前記電子マネーカードの前記ICメモリ部は、一対の個人公開鍵と個人秘密鍵を備え、

前記端末は、一対の端末公開鍵と端末秘密鍵を備え、

前記換金依頼電文は、取引に関する情報と前記電子マネーカードの前記個人秘密鍵を用いて生成された第1の認証子と、前記取引に関する情報と前記端末の前記端末秘密鍵を用いて生成された第2の認証子と、前記個人公開鍵と、前記端末公開鍵とを含み、

前記銀行コンピュータは、前記個人公開鍵と前記端末公開鍵を用いて前記第1と第2の認証子が一致するか否かを判別し、一致する場合にのみ、換金を行うための処理を実行する、

ことを特徴とする請求項1乃至12のいずれか1項に記載の電子マネーシステム。

【請求項14】前記電子マネーカードの追記型記憶部に記憶される取引履歴情報は、該電子マネーカードを特定する情報を含まない、ことを特徴とする請求項1乃至13のいずれか1項に記載の電子マネーシステム。

【請求項15】前記電子マネーカードの前記ICメモリ部と前記追記型記憶部の一方は、使用者の身体的特徴を示す特徴データを記憶しており、

前記端末は、操作者の身体的特徴を示す特徴データを取

4

得する取得手段と、前記電子マネーカードから前記特徴データを読み込む読込手段と、前記取得手段により取得された特徴データと前記読込手段により読み込まれた特徴データとを比較し、実質的に一致するか否かを判別する判別手段と、前記判別手段が実質的に一致すると判断した時に、該端末を介した電子マネーの取引を可能とし、前記判別手段が実質的に一致しないと判断した時に、該端末を介した電子マネーの取引を禁止する取引制御手段と、を備える、

10 ことを特徴とする請求項1乃至14のいずれか1項に記載の電子マネーシステム。

【請求項16】前記電子マネーカードの前記追記型記憶部は、光エネルギーが照射されることにより物理的にビットが形成されてデータが書き込まれ、書き換えが不可能な光記憶部から構成されている、ことを特徴とする請求項1乃至15のいずれか1項に記載の電子マネーシステム。

【請求項17】複数の端末と、該複数の端末と通信回線で接続されたセンタと、前記センタに通信回線で接続された銀行コンピュータと、より構成される電子マネーシステムであって、

該電子マネーシステムは、取引に関する情報を記憶する電子マネー取引ファイルを備え、

前記端末は、換金を含む電子マネーの取引の指示と取引金額を入力するための入力手段と、前記入力手段により入力された取引の指示のうちの換金指示と取引金額に基づいた換金依頼電文を前記センタに送信する換金依頼送信手段と、前記センタからの換金終了電文に回答して前記電子マネー取引ファイルに該換金処理に関する取引履歴を書き込む手段と、を備え、

前記センタは、前記端末からの前記換金依頼電文に基づいた振替指示電文を前記銀行コンピュータに送信する手段と、前記銀行コンピュータからの振替完了電文に回答して、前記端末に前記換金終了電文を送信する手段と、を備え、

前記銀行コンピュータは、前記センタからの前記振替指示電文により指示された取引金額を所定口座から該振替指示電文により特定された口座に振り替える振替手段と、前記振替手段による振替が完了すると前記振替完了電文を前記センタに送信する手段と、を備える、

40 ことを特徴とする電子マネーシステム。

【請求項18】前記電子マネー取引ファイルは、追記型記憶部とICメモリ部を備える媒体に記憶される、ことを特徴とする請求項17に記載の電子マネーシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、金銭的情報である電子マネーを取引する電子マネーシステムに関する。

【0002】

50 【従来の技術】貨幣的価値を有する金銭データを用いて

電子的な決済を可能とする電子マネーシステムが例えば、特公平7-111723等に開示されている。

【0003】

【発明が解決しようとする課題】電子マネーシステムでは、権限を有していない者の使用、金銭データのコピー、偽造等を有効に防止する必要がある。また、偽造等された金銭データの使用を発見した場合には、その流通経路を追跡し、不正元・偽造元等を発見できることが望ましい。しかし、このような要請を満たす電子マネーシステムは、未だに、提案されていない。

【0004】本発明は、上記実状に鑑みてなされたもので、金銭データの偽造等を有効に防止することができる電子マネーシステムを提供することを目的とする。また、本発明は、不正な取引を容易に検出し、その追跡性に優れた電子マネーシステムを提供することを目的とする。

【0005】

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点に係る電子マネーシステムは、追記型記憶部とICメモリ部とを備え、金銭的価値に関する情報を格納する電子マネーカードと、前記電子マネーカードを処理する端末と、前記端末と通信回線で接続され、前記端末を制御するセンタと、前記センタに通信回線で接続された銀行コンピュータと、より構成される電子マネーシステムであって、前記電子マネーカードの前記追記型記憶部は取引履歴情報を記憶し、前記電子マネーカードの前記ICメモリ部は、前記追記型記憶部に記憶された取引履歴情報の位置を示す位置情報を記憶し、前記端末は、換金を含む電子マネーの取引の指示と取引金額を入力するための入力手段と、前記入力手段により入力された前記取引の指示のうちの換金指示と取引金額に基づいた換金依頼電文を前記センタに送信する換金依頼送信手段と、前記センタからの換金終了電文にตอบสนองし、前記電子マネーカードの前記ICメモリ部に格納された前記位置情報に従って、該換金処理に関する取引履歴情報を前記電子マネーカードの前記追記型記憶部に書き込む手段と、を備え、前記センタは、前記端末からの前記換金依頼電文を受信し、受信した該換金依頼電文に基づいた振替指示電文を前記銀行コンピュータに送信する手段と、前記銀行コンピュータからの振替完了電文にตอบสนองして、前記端末に前記換金終了電文を送信する手段と、を備え、前記銀行コンピュータは、前記センタからの前記振替指示電文により指示された取引金額を所定口座から該振替指示電文により特定された口座に振り替える振替手段と、前記振替手段による振替が完了すると前記振替完了電文を前記センタに送信する手段と、を備える、ことを特徴とする。

【0006】このような構成によれば、利用者は電子マネーカードに格納された電子マネーを自己の口座に振替えることにより、電子マネーを換金することができる。しか

も、追記型記憶部に取引履歴を記録するので、異常が発生した場合に、この追記型記憶部の記録内容を検証し、不正行為等を容易に検出することができる。

【0007】前記電子マネーカードの前記追記型記憶部と前記ICメモリ部の少なくとも一方は、口座を特定するための口座特定情報を記憶してもよく、前記換金依頼送信手段は、前記電子マネーカードに記憶された前記口座特定情報を読み出し、前記換金依頼電文に含ませる手段を更に備えてもよい。口座特定情報としては、口座番号自体でもよく、或いは、口座番号と対応する他の番号、例えばカードID等でもよい。

【0008】前記端末に、前記電子マネーカードが保有している残高が前記入力手段により入力された前記取引金額以上か否かを判別し、前記残高が前記取引金額未満ならば、エラーメッセージを表示すると共に取引を中止若しくは金額の再入力を要求する手段を配置してもよい。また、前記センタは、例えば、前記電子マネーカードの残高を記憶する残高記憶手段と、前記電子マネーカードから受信した前記換金依頼電文により指示された取引金額を前記残高記憶手段に記憶されている該電子マネーカードの残高より差し引く残高更新手段と、を備える。この場合、センタは、前記電子マネーカードから受信した前記換金依頼電文により指示された取引金額が前記残高記憶手段に記憶されている該電子マネーカードの残高以下か否かを判別し、前記残高が前記取引金額未満ならば、取引の中止若しくは金額の再入力を指示する指示電文を前記端末に送信する手段と、を備えてもよい。このような構成とすることにより、取引の安全性を高めることができる。

【0009】前記取引履歴情報は、各取引について、取引の種別と、取引年月日と、その取引を処理した前記端末を特定する情報と、取引金額とを含む。これらの情報を追跡することにより、不正箇所を判別することができる。この場合前記追記型記憶部に、該電子マネーカードで取引された全ての取引履歴を記憶させることが望ましい。

【0010】前記センタに、前記電子マネーカードで取引された全ての取引履歴を記憶させてもよい。

【0011】前記電子マネーカードの前記追記型記憶部と前記ICメモリ部との少なくとも一方はその電子マネーカードのカード識別符号を記憶し、前記換金依頼電文は、前記電子マネーカードの前記カード識別符号を含み、前記センタは、使用を認めない前記電子マネーカードの前記カード識別符号を不正カードIDとして記憶する不正カードID記憶手段と、前記換金依頼電文に含まれる前記カード識別符号と前記不正カードID記憶手段に記憶されている前記不正カードIDとを比較し、一致する不正カードIDを検出すると、取引を中止する手段を備えてもよい。このような構成によれば、登録された事故カード等が使用された場合、それを検出し、取引を

中止できる。

【0012】前記端末は、端末識別符号を記憶し、前記換金依頼電文は、前記端末識別符号を含み、前記センタは、使用を認めない前記端末の前記端末識別符号を不正端末IDとして記憶する不正端末ID記憶手段と、前記換金依頼電文に含まれる前記端末識別符号を前記不正端末ID記憶手段に記憶される前記不正端末IDと比較し、一致する不正端末IDを検出すると、取引を中止する手段を備えてもよい。このような構成によれば、登録された事故端末等が使用された場合、それを検出し、取引を中止できる。

【0013】前記電子マネーカードに個人公開鍵及び／又はカード識別符号を付与し、前記個人公開鍵及び／又はカード識別符号がシステムに登録されているか否かを判別する認証局を配置してもよい。

【0014】前記電子マネーカードの前記ICメモリ部は、一対の個人公開鍵と個人秘密鍵を備え、前記端末は、一対の端末公開鍵と端末秘密鍵を備え、前記換金依頼電文は、取引に関する情報と前記電子マネーカードの前記個人秘密鍵を用いて生成された第1の認証子と、前記取引に関する情報と前記端末の前記端末秘密鍵を用いて生成された第2の認証子と、前記個人公開鍵と、前記端末公開鍵とを含み、前記銀行コンピュータは、前記個人公開鍵と前記端末公開鍵を用いて前記第1と第2の認証子が一致するか否かを判別し、一致する場合にのみ、換金を行うための処理を実行してもよい。このような構成によれば、電子マネーカードの不正使用をより正確に検出することができる。

【0015】前記電子マネーカードの追記型記憶部に記憶される取引履歴情報は、該電子マネーカードを特定する情報を含まないようにしてもよい。このような構成によれば、追記型記憶部の容量を有効に使用することができる。

【0016】操作者がこの電子マネーシステムを使用する権限を有しているか否かを、操作者の身体的特徴に基づいて判断してもよい。

【0017】前記追記型記憶部は、例えば、光エネルギーが照射されることにより物理的にビットが形成されてデータが書き込まれ、書き換えが不可能な光記憶部から構成される。

【0018】また、この発明の第2の観点に係る電子マネーシステムは、複数の端末と、該複数の端末と通信回線で接続されたセンタと、センタに通信回線で接続された銀行コンピュータと、より構成される電子マネーシステムであって、該電子マネーシステムは、金銭的価値に関する情報を記憶する電子マネー取引ファイルを備え、前記端末は、換金を含む電子マネーの取引の指示と取引金額を入力するための入力手段と、前記入力手段により入力された取引の指示のうちの換金指示及び取引金額に基づいた換金依頼電文を前記センタに送信する手段と、

前記センタからの換金終了電文に回答して前記電子マネー取引ファイルに該換金処理に関する取引履歴を書き込む手段と、を備え、前記センタは、前記端末からの前記換金依頼電文に基づいた振替指示電文を前記銀行コンピュータに送信する手段と、前記銀行コンピュータからの振替完了電文に回答して、前記端末に前記換金終了電文を送信する手段と、を備え、前記銀行コンピュータは、前記センタからの前記振替指示電文により指示された取引金額を所定口座から該振替指示電文により特定された口座に振り替える振替手段と、前記振替手段による振替が完了すると前記振替完了電文を前記センタに送信する手段と、を備える。

【0019】このような構成によれば、利用者は電子マネー取引ファイルに記憶された電子マネーを自己の口座に振り替えることにより、実質上、電子マネーを換金することができる。

【0020】また、前記電子マネー取引ファイルを、追記型記憶部とICメモリ部を備える媒体に記憶するようにしてもよい。この場合、追記型記憶部に取引履歴を記録することにより、異常が発生した場合に、この追記型記憶部の記録内容を検証し、不正行為等を容易に検出することができる。前記媒体は、カード、箱、円盤、ノート、手帳等、任意の形状をとり得る。また、前記電子マネー取引ファイルを記憶する前記媒体を、前記端末内に配置してもよい。

【0021】

【発明の実施の形態】以下、この発明の実施の形態にかかる電子マネーシステムを図面を参照して説明する。この電子マネーシステムは、図1に示すように、センタ10に配置されている認証局11及び電子マネーサーバ13と、電子マネー端末（取引装置）15と、銀行センタ17と、電子マネーカード19と、より構成される。

【0022】センタ10は、この電子マネーシステム全体の動作、電子マネーの流通を制御（管理）するコンピュータシステムである。センタ10の認証局11は、この電子マネーシステムにおける利用者等に対して認証情報を生成する。認証局11は、認証を行う際、利用者が登録されていることをチェックするため、このシステムにおいて使用される全ての電子マネーカード19のカードID及び公開鍵を記憶する。

【0023】電子マネーサーバ13は、一対のセンタ秘密鍵Ck1とセンタ公開鍵Ck2を生成し、認証局11にセンタ秘密鍵Ck1をコピーすることにより、センタ秘密鍵Ck1をセンタ10内で共有化する。また、電子マネーサーバ13は、センタ公開鍵Ck2を各電子マネー端末15等に予め配布する。また、電子マネーサーバ13は、後述する個人認証情報に含まれる署名を生成するための署名鍵Skと、その署名鍵Skを用いてなされた署名を確認するための検査鍵Ekとを生成、記憶し、検査鍵Ekを各電子マネー端末15に予め配布しておく。

【0024】電子マネーサーバ13は、図2、図3に示すように、各電子マネーカード19が保持する電子マネーの残高を示す残高テーブル、使用不可になった電子マネーカード19のカードIDのリスト（事故カードリスト）、使用不可になった電子マネー端末15の端末IDのリスト（事故端末リスト）、電子マネーの取引の履歴のリスト（取引履歴テーブル）を記憶する。

【0025】電子マネーサーバ13は、これらの記憶データを用いて、認証局11への認証要求、銀行センタ17への振替要求、各電子マネーカード19及び電子マネー端末15及び電子マネーの取引の制御・管理を行う。

【0026】電子マネー端末15は、利用者が電子マネーカード19を挿入又は装着し、所定の操作をすることにより、電子マネーの取引をするための端末である。電子マネー端末15には、電子マネーを電子マネーカード19に補充（チャージ）するためのチャージ端末（ATM等）、電子マネーカード相互間の電子マネーの授受を処理する端末、店舗等に配置され、物品やサービスの売り上げ金額に相当する電子マネーを受領するPOS端末、自動販売機等がある。1つの端末が電子マネーに関する複数の機能、例えば、ATM機能とPOS機能を備えている場合もある。

【0027】各電子マネー端末15は、記憶部30と、入力部31と、表示部32と、カード処理部33とを備える。

【0028】記憶部30は、その電子マネー端末15に付与された端末IDと、その電子マネー端末が生成した一対の端末秘密鍵Tk1及び端末公開鍵Tk2と、前述の電子マネーサーバ13より供給された個人認証情報確認用の検査鍵Ek及びセンタ公開鍵Ck2とセンタ10とのオフライン時の電子マネーの取引履歴等を格納する。

【0029】入力部31は、電子マネー取引の指示を入力する。表示部32は、処理メニュー、メッセージ等を表示する。カード処理部33は、電子マネーカード19を受け付ける挿入口と、電子マネーカード19のIC部20をアクセスするためのICリード／ライト部と、光記憶部21をアクセスするための光記憶リード／ライト部とを備える。

【0030】図4（A）にATM型の電子マネー端末15の例を示す。この電子マネー端末15の入力部31と表示部32は、タッチパネル型の表示部34から構成され、カード処理部33は、電子マネーカード19が挿入されるカード挿入口35Aと35Bを備える。カード挿入口35Aは、通常の処理と電子マネーの譲渡の際の譲渡元のカードが挿入される。カード挿入口35Bは、電子マネーの譲渡の際の譲渡先のカードが挿入される。

【0031】図4（B）にPOS型の電子マネー端末15の例を示す。この電子マネー端末15の入力部31は、電子マネーの取引の指示等と共に売り上げ金額など

を入力するためのキーボード31Aとバーコードリーダー31B等を含む。また、表示部32は、電子マネー取引のためメッセージ等と共に売り上げ金額などを表示し、顧客用の表示部32Aと操作者用の表示部32Bを備える。また、カード処理部33はカード挿入口35を備える。さらに、POS用に金銭ドロア36等も配置されている。

【0032】銀行センタ17は、電子マネーカード19の利用者（保有者）の口座である決済口座と銀行が保有する電子マネーの運用口座である別段口座を備え、これらの口座の入出金処理を行う。例えば、銀行センタ17は、センタ10からの指示に応じて電子マネーカード19に対応する決済口座から別段口座への振り替え及び別段口座から決済口座への振り替えを行う。この振り替え処理を行うため、銀行センタ17は、各電子マネーカード19に付与されているカードIDと各電子マネーカード19の利用者（保有者）の決済口座の口座番号を対応させる口座テーブルを図5に示すように記憶する。

【0033】電子マネーカード19は、図6に示すように、IC部（ICチップ）20と光記憶部21を備える光ICハイブリッドカードから構成される。なお、電子マネーカード19は、IC部（ICチップ）20と光記憶部21を備えていればよく、その形状はカード型に限定されず、ノート、手帳、箱、円盤等、種々の形状が可能である。

【0034】IC部20は制御回路とメモリ回路を内蔵する。このメモリ回路は、図6に示すように、動作プログラムの他に、カードID、個人秘密鍵Pk1、個人公開鍵Pk2、電子マネーの残高、後述するオンライン取引用の個人認証情報、等を記憶する。また、IC部20は、後述する光記憶部21に記憶される取引履歴のうち、最終的な取引履歴の位置を示す最終取引ポイントと、電子マネーサーバ13へ最後に送信した取引履歴の位置を示す送信済みポイントを記憶する。

【0035】光記憶部21は、例えば、光エネルギーが照射されることによりビット等が形成されてデータが書き込まれるタイプの書き換え不可能な追記型の記憶媒体等から構成され、電子マネーカード19で取り引きされた電子マネーの取引履歴を順次記憶する。

【0036】取引履歴を構成する項目としては、電子マネーの取引の種別を示す利用区分（チャージ（残高の補充）、支払、譲渡、換金等）、取引のために電子マネーカードが装着された電子マネー取引端末15の端末ID、電子マネーカード19間の電子マネーの授受の場合には相手のカードID、利用年月日、取引金額、認証子（上記項目と個人秘密鍵Pk1を用いて作成した取引認証子、上記項目と取引相手（電子マネー端末15又は他の電子マネーカード19）の秘密鍵Pk1を用いて作成した取引先認証子）、等がある。

【0037】このような構成を有する電子マネーシステ

ムにおける基本的な処理には、(1) 電子マネーチャージ処理(電子マネーカード19に記憶される残高の補充)、(2) 個人認証情報発行処理、(3) 電子マネー支払い処理、(4) 突き合わせ処理、(5) 電子マネー譲渡処理、(6) 電子マネー換金処理、等がある。これらの処理について、以下順番に説明する。

【0038】(1) 電子マネーチャージ処理

電子マネーチャージ処理を図7を参照して説明する。ATM機能を備える電子マネー端末15は、図8(A)に示すように、処理選択メニューを表示している。利用者は、表示部32(タッチパネル34)に表示されている処理メニューの中から「1) 電子マネーのチャージ」を選択する。

【0039】この選択に応答し、電子マネー端末15は、図8(B)に示すように、電子マネーカード19をカード挿入口35Aに挿入すべき旨のメッセージを表示する。

【0040】電子マネー端末15は、電子マネーカード19が挿入されると、図8(C)に示すような金額入力画面を表示し、利用者は入力部31(タッチパネル34)から所望のチャージ金額を入力する。チャージ金額が入力されると電子マネー端末15は、電子マネーカード19に、取引区分(チャージ)と利用年月日と取引金額(チャージ金額)とから構成される取引情報と端末IDと、カードIDと個人公開鍵Pk2の送信を要求する要求信号を送信する(P1)。

【0041】電子マネーカード19のIC部20は、端末IDと取引情報に、カードIDを加え、これらの情報を個人秘密鍵Pk1を用いて取引認証子{Pk1(端末ID+取引情報+カードID)}に変換し、その取引認証子とカードIDと個人公開鍵Pk2とを電子マネー端末15に送信する(P2)。

【0042】電子マネー端末15は、受信したカードIDに取引情報と端末IDを加え、端末秘密鍵Tk1を用いて取引先認証子{Tk1(端末ID+取引情報+カードID)}を作成する。電子マネー端末15は、作成した取引先認証子{Tk1(端末ID+取引情報+カードID)}と、要求された金額のチャージを指示し、端末公開鍵Tk2を含むチャージ要求電文と、電子マネーカード19のカードIDと、個人公開鍵Pk2と、取引認証子とを電子マネーサーバ13に送信する(P3)。なお、チャージ要求電文は、送信元の電子マネー端末15の端末IDを含む。

【0043】電子マネーサーバ13は、受信したカードID及び端末IDが、記憶部30に記憶している事故カードリスト(図2(B))及び事故端末リスト(図2(C))に登録されているかを判別する。受信したカードID及び端末IDが、これらのリストに登録されていないと判別された場合、電子マネーサーバ13は、受信した個人公開鍵Pk2を用いて取引認証子{Pk1(端

末ID+取引情報+カードID)}を端末IDと取引情報とカードIDとに変換する。又、受信した端末公開鍵Tk2を用いて取引先認証子{Tk1(端末ID+取引情報+カードID)}を端末IDと取引情報とカードIDに変換する。さらに、取引認証子から変換された端末IDと取引情報とカードIDと、取引先認証子から変換された端末IDと取引情報とカードIDとが一致するか否かを判別する。これらが完全に一致した場合、電子マネーサーバ13は、この取引認証子と取引先認証子は正しいと判別し、そのカードIDに対応する決済口座から銀行センタ17の別段口座へ指示された金額を移動する(出金する)よう指示する出金電文を銀行センタ17に送信する(P4)。

【0044】なお、受信したカードIDと端末IDの少なくとも一方が事故カードリスト及び事故端末リストに登録されている場合、又は取引認証子と取引先認証子から変換された端末IDと取引情報とカードIDとの少なくとも一部が一致しない場合、電子マネーサーバ13は、電子マネー端末15にチャージ不可を指示するメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者等に通知する。電子マネー端末15はチャージをできない旨のメッセージを表示部32に表示する。

【0045】銀行センタ17は、電子マネーサーバ13より、出金電文を受信すると、図5に示す口座テーブルを参照して、カードIDに対応する口座番号を判別する。次に、この口座番号の決済口座の残高をチェックし、残高が指示された金額以上であるかを判別する。残高が指示された金額以上であると判別した場合、出金可能と判別し、決済口座から別段口座に指示された所定金額を移動する(振り替える)(P5)。次に、振替完了を通知する出金完了電文を電子マネーサーバ13に送信する(P6)。

【0046】決済口座の残高の不足により出金不可能な場合には、銀行センタ17は、チャージ不可を指示する電文を電子マネーサーバ13に送信する。電子マネーサーバ13はチャージ処理を中止すると共に電子マネー端末15に同様のメッセージを送信する。電子マネー端末15はこのメッセージに応答して、その旨を示すメッセージを表示部32等に表示する。

【0047】電子マネーサーバ13は、出金完了電文を銀行センタ17から受信すると、記憶部30に記憶していた電子マネーカード19のカードID及び個人公開鍵Pk2を認証局11へ送信し、それらに対する認証情報を要求する(P7)。認証局11は、自己が記憶するカードID及び個人公開鍵Pk2のリストに、受信したカードID及び個人公開鍵Pk2が登録されているかをチェックする。それらが登録されているならば、認証局11は、センタ秘密鍵Ck1を用いて、受信したカードID及び個人公開鍵Pk2を認証情報{Ck1(カードID+Pk2)}

に変換し、認証完了電文と共に電子マネーサーバ13へ返送する(P8)。

【0048】電子マネーサーバ13は、認証完了電文及び認証情報{Ck1(カードID+Pk2)}を受信すると、図2(A)に示す残高テーブル上で、電子マネーカード19にチャージされている電子マネーの残高を示す残高データを更新する。さらに、図3に示すように、取引情報(利用区分(チャージ)、利用年月日、取引金額)とカードIDと端末IDと認証子(取引認証子と取引先認証子)より構成される今回の取引履歴を過去の取引履歴に追加して記憶する。次に、電子マネーサーバ13は、認証局11からの認証情報を今回の取引履歴に付与し、チャージの完了を示すチャージ完了電文と共に電子マネー端末15に送信する(P9)。

【0049】電子マネー端末15は、取引履歴と認証情報を受信すると、センター公開鍵Ck2を用いて認証情報をカードIDと個人公開鍵Pk2に変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴に基づいて、IC部20の制御部を介して、IC部20のメモリエリアに記録されている残高を

更新する。
【0050】また、電子マネー端末15は、IC部20より最終取引ポイントを読み出し、最終取引ポイントが指示する位置の次のアドレス位置に今回の取引履歴(取引情報(利用区分(チャージ)、利用年月日、取引金額)とカードIDと端末IDと認証子(取引認証子と取引先認証子))を過去の取引履歴に追加して記憶する。さらに、電子マネー端末15は、IC部20の制御部を介して、IC部20のメモリエリアに記録されている最終取引ポイント及び送信済みポイントが追記した取引履歴の位置を指すように更新する(P10)。その後、端末15はチャージが完了した旨を表示部32に表示すると共に電子マネーカード19を排出する。

【0051】この電子マネーチャージ処理を、利用者Aが、電子マネー端末15B(端末ID" T150")を用いて、自己の電子マネーカード19A(カードID" C99")に1万円分の電子マネーをチャージする場合を例に、図9を参照して説明する。まず、利用者Aは、表示部32に表示された処理メニューから「1) 電子マネーのチャージ」を選択し、電子マネーカード19Aを電子マネー端末15Bに挿入し、チャージ金額として「1万円」を入力する。

【0052】電子マネー端末15Bは、この入力に回答し、取引区分(チャージ)と利用年月日と取引金額とから構成される取引情報と端末ID" T150"とを、カードIDと個人公開鍵Pk2を要求する要求信号と共に電子マネーカード19Aに送信する(L1)。

【0053】電子マネーカード19Aは、受信した端末ID" T150"と取引情報にカードID" C99"を加え、個人秘密鍵Pk1Aを用いて取引認証子{Pk1A

(T150+取引情報+C99)}を作成する。電子マネーカード19Aは、作成した取引認証子{Pk1A(T150+取引情報+C99)}をカードID" C99"と個人公開鍵Pk2Aと共に電子マネー端末15Bに送信する(L2)。

【0054】電子マネー端末15Bは、カードID" C99"と記憶部30に記憶していた取引情報に端末IDを加え、端末秘密鍵Tk1Bを用いて取引先認証子{Tk1B(T150+取引情報+C99)}を作成する。電子マネー端末15Bは、作成した取引先認証子{Tk1B(T150+取引情報+C99)}と、1万円分の電子マネーのチャージを要求すると共に端末ID" T150"と端末公開鍵Tk2Bを含むチャージ要求電文と、電子マネーカード19AのカードID" C99"と、個人公開鍵Pk2Aと、取引認証子{Pk1A(T150+取引情報+C99)}とを、電子マネーサーバ13に送信する(L3)。

【0055】電子マネーサーバ13は、受信した端末ID" T150"とカードID" C99"が、事故端末リスト及び事故カードリストに登録されているか否かを判別することにより、電子マネー端末15及び電子マネーカード19の不正使用をチェックする。

【0056】チェックの結果、電子マネーカード19A及び電子マネー端末15Bが事故カードと事故端末のいずれでもないと判別されたならば、電子マネーサーバ13は、個人公開鍵Pk2Aを用いて取引認証子を端末IDと取引情報とカードIDとに変換する。又、端末公開鍵Tk2Bを用いて取引先認証子を端末IDと取引情報とカードIDとに変換する。次いで、取引認証子から変換された端末IDと取引情報とカードIDと、取引先認証子から変換された端末IDと取引情報とカードIDとが完全に一致するか否かを判別する。これらが完全に一致した場合、電子マネーサーバ13は、この取引認証子と取引先認証子は正しいと判別し、銀行センタ17へカードID" C99"の決済口座から銀行センタ17の別段口座へ1万円を移動するよう指示する出金電文を送信する(L4)。

【0057】電子マネーカード19Aと電子マネー端末15Bの両方又は一方が事故カード又は事故端末であると判別された場合、及び/又は、取引認証子と取引先認証子から変換された端末IDと取引情報とカードIDとが互いに一致しない場合、電子マネーサーバ13は、電子マネー端末15Bにチャージできない旨のメッセージを送信すると共に、不正又は異常の検出を管理者に通知する。

【0058】銀行センタ17は、出金電文を受信すると、図5に示す口座テーブルを参照してカードID" C99"の決済口座の口座番号"300000001"を検索し、該当する口座番号の残高が、指示されたチャージ金額の1万円以上か否かを判別する。残高が1万円未満

の場合は、銀行センタ17は、残高不足のためチャージできないの旨の電文を電子マネーサーバ13に送信する。残高が1万円以上の場合、銀行センタ17は、決済口座"30000001"から銀行センタ17の別段口座へ1万円を移動し、出金完了電文を電子マネーサーバ13に送信する(L5)。

【0059】電子マネーサーバ13は、銀行センタ17から出金完了電文を受信すると、電子マネーカード19AのカードIDと個人公開鍵Pk2Aに対して認証を要求する認証付与要求を、カードID" C99"と個人公開鍵Pk2Aと共に認証局11へ送信する(L6)。

【0060】認証局11は、自己が記憶している電子マネーカード19AのカードID及び個人公開鍵Pk2のリストに、受信したカードID" C99"と個人公開鍵Pk2Aが存在する(即ち、認証局11に登録されている)ことをチェックする。カードID" C99"と個人公開鍵Pk2Aとが認証局11に登録されている場合、認証局11は、センタ秘密鍵Ck1を用いて、受信したカードID" C99"と個人公開鍵Pk2Aに対する認証情報{Ck1(C99+Pk2A)}を生成し、認証の完了を示す認証完了電文と共に電子マネーサーバ13に送信する(L7)。

【0061】電子マネーサーバ13は、認証完了電文を受信すると、利用区分"チャージ"、利用年月日、カードID" C99"、端末ID" T150"、チャージ金額"1万円"、取引認証子、取引先認証子、等により取引履歴を生成して図3に示すように記憶する。また、図2(A)に示す残高テーブルのカードID" C99"の残高に1万円加算する。さらに、生成した取引履歴に認証局11からの認証情報を付与して、チャージ完了電文と共に電子マネー端末15Bに送信する(L8)。

【0062】電子マネー端末15Bは、認証情報が付与された取引履歴を受信すると、センタ公開鍵Ck2を用いて認証情報{Ck1(C99+Pk2A)}をカードID" C99"と個人公開鍵Pk2Aに変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴を電子マネーカード19AのIC部20に送信する(L9)。IC部20は、受信した取引履歴に基づいて、自己が記憶している残高に1万円を加算する。

【0063】また、電子マネー端末15Bは、IC部20から最終取引ポイントを読み出し、光記憶部21の最終取引ポイントが示す位置の次の位置に取引履歴を追記し、最終取引ポイント及び送信済みポイントを追記された取引履歴を示すように更新する。その後、端末15Bはチャージが完了した旨を表示部32に表示すると共に電子マネーカード19Aを排出する。このようにして、利用者Aは自己の電子マネーカード19Aに、1万円分の電子マネーをチャージすることができる。

【0064】(2)個人認証情報発行処理次に、電子マ

ネーカード19のIC部20に記憶される個人認証情報の発行処理(個人認証情報発行処理)について説明する。後述するオフラインによる電子マネー支払い処理において、電子マネーカード19は、この個人認証情報を電子マネー端末15に提示し、電子マネー端末15によりその個人認証情報の確認を受けることで、取引することが可能となる。個人認証情報は、電子マネーカード19のカードID及び個人公開鍵Pk2をもとに作成されるため、個人秘密鍵Pk1及び個人公開鍵Pk2が変更される度に取得される必要がある。

【0065】図10に個人認証情報発行処理の概要図を示す。まず、図8(A)に示すように、表示部32に表示される処理メニューから「4)個人認証情報の発行」が選択され、電子マネーカード19が電子マネー端末15に挿入される。電子マネー端末15は、この操作に回答して、電子マネーカード19のIC部20にカードIDと個人公開鍵Pk2の要求を示す要求信号を送信する(P11)。

【0066】この要求信号に回答して、電子マネーカード19のIC部20は、カードIDと個人公開鍵Pk2を電子マネー端末15に送信する(P12)。電子マネー端末15は、受信したカードIDと個人公開鍵Pk2とを、個人認証情報を要求する認証情報発行要求と共に電子マネーサーバ13に送信する(P13)。なお、認証情報発行要求は端末IDを含む。

【0067】電子マネーサーバ13は、電子マネー端末15からカードIDと個人公開鍵Pk2と認証情報発行要求を受信すると、受信したカードID及び端末IDが事故カードIDリスト及び事故端末IDリストに登録されているか否かをチェックする。

【0068】チェックの結果、受信したカードIDと端末IDの少なくとも一方が事故カードIDリスト又は事故端末IDリストに登録されている場合、電子マネーサーバ13は、電子マネー端末15に個人認証情報を発行できない旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。電子マネー端末15はこのメッセージを表示する。

【0069】受信したカードID及び端末IDが事故カードIDリスト及び事故端末IDリストに登録されていない場合、電子マネーサーバ13は、受信したカードIDと個人公開鍵Pk2と個人認証情報の発行要求(個人認証情報発行要求)を認証局11に送信する(P14)。

【0070】認証局11は、電子マネーサーバ13からカードIDと個人公開鍵Pk2と個人認証情報発行要求を受信すると、受信したカードID及び個人公開鍵を本システムにおいて使用可能なものとして登録する。

【0071】受信したカードIDと個人公開鍵Pk2を登録した後、認証局11は署名鍵Skを用いて作成(暗号化)した署名Sk(カードID+Pk2)をカードIDと個人公開鍵Pk2に付与することにより、個人認証情報

{ (カードID+Pk2) + Sk (カードID+Pk2) } を生成し、発行完了電文と共に電子マネーサーバ13に送信する(P15)。なお、(カードID+Pk2)を圧縮し、更にハッシュ関数を用いて変換したデータを署名鍵Skで暗号化したものを署名として用いてもよい。

【0072】電子マネーサーバ13は、認証局11からの個人認証情報 { (カードID+Pk2) + Sk (カードID+Pk2) } と発行完了電文を電子マネー端末15へ送信する(P16)。電子マネー端末15は、受信した個人認証情報 { (カードID+Pk2) + Sk (カードID+Pk2) } を電子マネーカード19のIC部20へ送信する(P17)。IC部20は、受信した個人認証情報 { (カードID+Pk2) + Sk (カードID+Pk2) } を記憶回路に記憶する。その後、電子マネー端末15は、個人認証情報の取得が完了した旨を表示部32に表示すると共に電子マネーカード19を排出する。

【0073】この個人認証情報発行処理を、例えば、利用者Aが電子マネーカード19A(カードID" C99")の個人認証情報を取得する場合を例に、図11を参照して説明する。

【0074】まず、利用者Aは、表示部32に表示されたメニューの中から「4) 個人認証情報の発行」を選択し、電子マネーカード19Aを電子マネー端末15Bに挿入する。電子マネー端末15Bは、この操作にตอบสนองし、電子マネーカード19AにカードIDと個人公開鍵の送信を要求する要求信号を送信する(L11)。

【0075】電子マネーカード19AのIC部20は、電子マネー端末15Bからの要求信号を受信すると、カードID" C99"と個人公開鍵Pk2Aを電子マネー端末15Bに送信する(L12)。電子マネー端末15Bは、受信したカードID" C99"と個人公開鍵Pk2Aを認証情報発行要求と共に電子マネーサーバ13に送信する(L13)。

【0076】電子マネーサーバ13は、受信したカードID" C99"と個人公開鍵Pk2Aとが、事故カードIDリスト及び事故端末IDリストに登録されているか否かを判別することにより、電子マネーカード19及び電子マネー端末15の不正使用をチェックする。不正使用と判別された場合、電子マネーサーバ13は、電子マネー端末15Bに個人認証情報を発行できない旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。電子マネー端末15Bは、このメッセージを表示する。

【0077】チェックの結果、電子マネーカード19A及び電子マネー端末15Bが使用可能ならば、カードID" C99"と個人公開鍵Pk2Aを個人認証情報発行要求と共に認証局11へ送信する(L14)。

【0078】認証局11は、電子マネーサーバ13から受信したカードID" C99"と個人公開鍵Pk2Aをこのシステムにおいて使用可能なものとして登録する。カ

ードID" C99"と個人公開鍵Pk2Aの登録後、認証局11は、それらを署名鍵Skで暗号化することによりデジタル署名を生成し、カードID" C99"と個人公開鍵Pk2Aに付与することにより、個人認証情報 { (C99+Pk2A) + Sk (C99+Pk2A) } を生成し、発行完了電文と共に電子マネーサーバ13に送信する(L15)。

【0079】電子マネーサーバ13は、認証局11からの個人認証情報 { (C99+Pk2A) + Sk (C99+Pk2A) } と発行完了電文を電子マネー端末15に送信する(L16)。電子マネー端末15は、電子マネーサーバ13から受信した個人認証情報 { (C99+Pk2A) + Sk (C99+Pk2A) } を電子マネーカード19Aに送信する(L17)。電子マネーカード19AのIC部20は、電子マネー端末15から受信した個人認証情報 { (C99+Pk2A) + Sk (C99+Pk2A) } を記憶する。その後、電子マネー端末15Bは、個人認証情報の取得が完了した旨を表示部32に表示すると共に電子マネーカード19Aを排出する。

【0080】個人認証情報は、個人秘密鍵Pk1及び個人公開鍵Pk2が電子マネー端末15で変更された際に、自動的に該電子マネー端末15を介して取得されてもよい。

【0081】(3) 電子マネー支払い処理

次に、電子マネー支払い処理について図12を参照して説明する。この処理は、例えば、店舗等において商品、サービス等を購入し、その料金を電子マネーで支払うための処理である。電子マネー端末15は、例えば、図4(B)に示すようなPOS端末、自動販売機、等の形態をとる。

【0082】例えば、POS端末型電子マネー端末15で売り上げ額を計算した後、支払い方法を選択すべき旨のメッセージが表示部32に表示される。ここで、電子マネーカードによる支払いが選択されると、図8(B)に示すような電子マネーカード19を挿入すべき旨の指示が表示され、電子マネーカード19が電子マネー端末15に挿入される。

【0083】電子マネー端末15は、電子マネーカード19の挿入にตอบสนองして、取引区分と利用年月日と取引金額(支払い金額)とから構成される取引情報と端末IDと、カードIDと個人公開鍵Pk2と個人認証情報 { (カードID+Pk2) + Sk (カードID+Pk2) } と残高の送信を要求する要求信号を電子マネーカード19に送信する(P21)。

【0084】電子マネーカード19のIC部20は、受信した端末ID及び取引情報にカードIDを加え、個人秘密鍵Pk1を用いて取引認証子 { Pk1(端末ID+取引情報+カードID) } を作成する。IC部20は、作成した取引認証子 { Pk1(端末ID+取引情報+カードID) } をカードIDと個人公開鍵Pk2と個人認証情報

{ (カードID+Pk2) + Sk (カードID+Pk2) }
と残高とを電子マネー端末15に送信する(P22)。

【0085】電子マネー端末15は、電子マネーカード19からカードIDと個人公開鍵Pk2と個人認証情報 { (カードID+Pk2) + Sk (カードID+Pk2) } と残高と取引認証子 { Pk2 (端末ID+取引情報+カードID) } を受信すると、まず、個人認証情報 { (カードID+Pk2) + Sk (カードID+Pk2) } のうち、カードIDと個人公開鍵Pk2に付与されたデジタル署名 Sk (カードID+Pk2) を検査鍵Ekを用いて復号し、署名が付与されていたカードIDと個人公開鍵Pk2に一致するか否かを判別する。一致しない場合、電子マネー端末15は、何らかの不正があると判断し、取引不可のメッセージを表示し、不正検出を電子マネーサーバ13に通知する。

【0086】電子マネー端末15は、検査鍵Ekを用いて署名から復号されたカードIDと個人公開鍵Pk2が、署名が付与されていたカードIDと個人公開鍵Pk2に一致すると判断すると、受信した残高が支払金額以上か否かを判別する。残高が支払い金額以上ならば、支払可能と判断し、取引情報とカードIDと端末IDに対して端末秘密鍵Tk1を用いて取引先認証子 { Tk1 (端末ID+取引情報+カードID) } を生成する。電子マネー端末15は、取引情報とカードIDと端末IDと取引認証子 { Pk2 (端末ID+取引情報+カードID) } と取引先認証子 { Tk1 (端末ID+取引情報+カードID) } より取引履歴を構成し、支払い完了電文と共に電子マネーカード19に送信し(P23)、さらに、自己の記憶部30にも記憶する。

【0087】電子マネーカード19のIC部20は、受信した取引履歴に基づいて、記憶回路に格納している残高を更新すると共に最終履歴ポインタの値を電子マネー端末15に転送する。電子マネー端末15は、電子マネーカード19の光記憶部21の最終履歴ポインタが指示するアドレスの次のアドレスに取引履歴を書き込むと共にIC部20に最終履歴ポインタを更新するコマンドを送出する。このコマンドに回答して、IC部20は記憶回路に格納されている最終取引ポインタの値を更新する。ただし、送信済みポインタの値は更新しない。その後、電子マネー端末15は、支払いが完了した旨を表示すると共に電子マネーカード19を排出する。

【0088】上述したように、この電子マネー支払い処理は、電子マネーカード19と電子マネー端末15の間で処理されるオフライン処理である。これにより、処理速度を向上させ、レスポンスを速くし、顧客の待ち時間等を短縮することができる。

【0089】電子マネー端末15は、所定のタイミングで電子マネーサーバ13と通信を行い、記憶部30に蓄積していた取引履歴を送信する。電子マネーサーバ13は、受信した取引履歴を図3に示すように、取引履歴テ

ーブルに記憶する。電子マネー端末15が取引履歴を電子マネーサーバ13に送信するタイミングとしては、例えば、電子マネー支払い処理が完了した直後等のタイミングが望ましい。しかし、これに限定されるものではなく、たとえば、一定期間毎(例えば、10分毎)、電子マネーサーバ13からのポーリングに応じて等、任意である。

【0090】電子マネー端末15は、記憶部30に蓄積していた取引履歴を電子マネーサーバ13に送信した後、送信済みの取引履歴を消去してもよく、又、送信済みフラグ等を付与することにより、送信済みの取引履歴と未送信の取引履歴とを区別して管理してもよい。

【0091】電子マネー支払い処理を、例えば、利用者Aが、端末IDが" T150 " の電子マネー端末15Bが設置された店舗において1万円の商品を購入し、その支払いを電子マネーカード19A (カードID" C99 ") で行う場合を例に図13を参照して説明する。まず、電子マネー端末15B (例えばPOS端末) の表示部32に金額" 1万円 " が支払金額として表示され、利用者が電子マネーによる支払いを選択したとする。まず、利用者A又は店員が電子マネーカード19Aを電子マネー端末15Bに挿入する。

【0092】電子マネー端末15Bは、電子マネーカード19Aの挿入に回答して、取引区分と取引年月日と取引金額とから構成される取引情報と端末ID" T150 " と、カードID" C99 " と個人公開鍵Pk2と個人認証情報と残高の送信を要求する要求信号を電子マネーカード19Aに送信する(L21)。

【0093】電子マネーカード19Aは、受信した端末ID" T150 " と取引情報にカードID" C99 " を加え、個人秘密鍵Pk1Aを用いて取引認証子 { Pk1A (T150+取引情報+C99) } を作成する。電子マネーカード19Aは、作成した取引認証子 { Pk2A (T150+取引情報+C99) } と、カードID" C99 " と、個人公開鍵Pk2Aと、個人認証情報 { (C99+Pk2) + Sk (C99+Pk2) } と、残高とを電子マネー端末15に送信する(L22)。

【0094】電子マネー端末15Bは、電子マネーカード19Aから、カードID" C99 " と個人公開鍵Pk2Aと個人認証情報 { (C99+Pk2) + Sk (C99+Pk2) } と残高と取引認証子 { Pk1A (T150+取引情報+C99) } とを受信し、個人認証情報のうち、署名Sk (C99+Pk2) を、予め記憶している検査鍵Ekを用いて復号する。次に、復号されたものが、署名が付与されていた電子マネーカード19AのカードID" C99 " と個人公開鍵Pk2Aと一致することを確認する。

【0095】次に、電子マネー端末15Bは、電子マネーカード19Aの残高が支払い金額(この場合1万円)以上か否かを判別する。残高が1万円以上ならば、電子マネー端末15Bは、端末ID" T150 " と取引情報

とカードID" C99" に対して端末秘密鍵Tk1Bを用いて取引先認証子{Tk1B(T150+取引情報+C99)}を生成する。さらに、端末ID" T150" と取引情報とカードID" C99" と取引認証子{Pk1A(T150+取引情報+C99)}と取引先認証子{Tk1B(T150+取引情報+C99)}より取引履歴を構成し、支払い完了電文と共に電子マネーカード19Aへ送信する(L23)。また、取引履歴を自己の記憶部30にも記憶する。その後、電子マネー端末15Bは、支払いが完了した旨を表示すると共に電子マネーカード19Aを排出する。

【0096】電子マネーカード19AのIC部20は、電子マネー端末15Bから受信した取引履歴に基づいて、残高を1万円分減算すると共に最終取引ポイントの値を電子マネー端末15Bに送信する。電子マネー取引端末15Bは、光記憶部21の最終取引ポイントが示すアドレスの次のアドレスに取引履歴を格納する。その後、IC部20に最終読み出しポイントの値を次のアドレス位置を示すように更新する。ただし、送信済みポイントの値は更新しない。

【0097】一方、署名を検査鍵Ekにより復号したものが電子マネーカード19AのカードID" C99" と個人公開鍵Pk2Aと一致しないと判断された場合、電子マネー端末15Bは電子マネーカード19Aを不正カードと判別し、支払い不可の旨のメッセージを表示部32に表示すると共に、不正検出を電子マネーサーバ13に通知する。また、電子マネーカード19Aの残高が1万円未満の場合、電子マネー端末15Bは、残高不足のため支払い不可の旨のメッセージを表示部32に表示する。

【0098】電子マネー端末15Bは、記憶部30に記憶していた取引履歴を支払い処理終了後、電子マネーサーバ13に送信する。電子マネーサーバ13は取引履歴を受信すると、受信した取引履歴を図3に示すように、取引履歴テーブルに格納する。電子マネー端末15Bは、電子マネーサーバ13から取引履歴の記憶部30に蓄積していた取引履歴の送信完了後、送信済みの取引履歴を消去してもよく、又、送信済みフラグ等を付与することにより、送信済みの取引履歴と未送信の取引履歴とを区別して管理してもよい。

【0099】なお、以上の説明では、支払い処理をオフラインで行ったが、セキュリティを高めるため、取引金額が一定額以上の場合は、オンラインで処理するようにしてもよく、又、一回の取引限度額を定めてもよい。また、電子マネー端末15も電子マネーカード19の個人認証情報と同様の「端末認証情報」を備え、取引の際、自己の端末認証情報を電子マネーカード19に送信し、確認を受けるようにしてもよい。この場合、電子マネーカード19は、端末認証情報に含まれる署名を確認(検査)するための検査鍵を備える。このシステムでは、電

子マネーカード19と電子マネー端末15との間でそれぞれの個人認証情報と端末認証情報が正しいと相互に確認されたとき、取引が可能となるため、システムのセキュリティをより高めることができる。

【0100】(4) 突き合わせ処理

支払い処理等が実行されると、電子マネーカード19には、電子マネーサーバ13に対して未送信の取引履歴が発生する。これらの取引履歴は、オンラインで行われる処理(例えば、電子マネーのチャージ処理等)の実行時、その処理に先だって電子マネーサーバ13に送信される。電子マネーサーバ13は、電子マネーカード19から取引履歴を電子マネー端末15を介して受信すると、自己が記憶している取引履歴と突き合わせることにし、その正当性をチェックする。この突き合わせ処理の概要を図14を参照して説明する。

【0101】電子マネーカード19のIC部20は、電子マネー端末15からの信号を受信すると、受信した信号が指示する処理の内容を判別し、それがオンライン処理を指示しているか否かを判別する。

【0102】例えば、「1) 電子マネーのチャージ」が処理メニューの中から選択され、電子マネーカード19が電子マネー端末15に挿入され、金額が入力されると、電子マネー端末15は、例えば、チャージ処理を行うために、取引情報等を電子マネーカード19のIC部20に送信する(図7P1、図9のL1)。

【0103】IC部20は、指示された処理がオンライン処理であることを取引情報から判別し、IC部20の最終取引ポイントと送信済みポイントとが一致しているか否かを判別する。一致していないと判別した場合、IC部20は、割り込み信号と共に、送信済みポイントが示すポイントの次の位置から、最終取引ポイントが示す位置までの各アドレスに記憶されている取引履歴とカードIDと個人公開鍵Pk2を電子マネー端末15に送信する(P31)。

【0104】電子マネー端末15は、割り込み信号に応答し、受信したカードIDと個人公開鍵Pk2と取引履歴を電子マネーサーバ13に送信する(P32)。

【0105】電子マネーサーバ13は、受信したカードIDと個人公開鍵Pk2を、それらが認証局11に登録されていることの確認を要求する確認要求と共に認証局11に送信する(P33)。

【0106】認証局11は、受信したカードIDと個人公開鍵Pk2が、自己が記憶するカードIDと個人公開鍵のリストに登録されているか否かを判別する。登録されていることを確認すると、確認の完了を示す確認完了電文を電子マネーサーバ13に返送する(P34)。受信したカードIDと個人公開鍵Pk2が登録されていない場合、認証局11は、不正の検出を電子マネーサーバ13に通知する。

【0107】認証局11からの確認完了電文を受信する

と、電子マネーサーバ13は、電子マネーカード19から受信した取引履歴を自己が記憶している取引履歴と突き合わせる。受信した取引履歴と自己が記憶している取引履歴が全て一致し、突き合わせが完了すると、電子マネーサーバ13は、電子マネー端末15に突き合わせ完了電文を送信する(P35)。

【0108】電子マネー端末15は、受信した突き合わせ完了電文を電子マネーカード19に送信する(P36)。電子マネーカード19は、突き合わせ完了電文を受信すると、IC部20に記憶している送信済みポイントを最終取引ポイントと一致するように更新する。続いて、電子マネー端末15により本来要求されている処理を実行する。

【0109】電子マネーサーバ13は、受信した取引履歴と自己が記憶している取引履歴が一致しないと判断した場合、電子マネー端末15に突き合わせ不一致を通知すると共に、不正の検出をメッセージ表示等により管理者等に通知する。

【0110】なお、最終取引ポイントと送信済みポイントとが一致する場合、未送信履歴が存在しないため、電子マネーカード19は、要求信号に応じた処理を続行する。

【0111】この突き合わせ処理を、電子マネー支払処理がなされた後でだけ実行するようにしてもよい。この場合、例えば、電子マネー端末15は、電子マネー支払処理を実行すると、電子マネーカード19のIC部20に未送信履歴フラグをセットする。電子マネー取引端末15は、電子マネーカード19が挿入され、オンライン処理が指示されると、未送信履歴フラグがオンであるか否かを判別し、オンならば、上述の突き合わせ処理を実行する。

【0112】この突き合わせ処理を、図15、図16を参照して具体的に説明する。ここで、利用者Aは以前、カードID" C99"の電子マネーカード19Aで電子マネーの支払いをしており、電子マネーカード19Aの光記憶部21には未送信の取引履歴が記憶されていることとする。

【0113】利用者Aは、例えば、電子マネーのチャージを指示し、電子マネーカード19Aを電子マネー端末15Bに挿入する。電子マネー端末15Bは、取引区分(チャージ)と利用年月日と取引金額とから構成される取引情報と端末IDとを、カードIDと個人公開鍵Pk2を要求する要求信号と共に電子マネーカード19AのIC部20に送信する。

【0114】IC部20は、取引情報から、オンライン処理が選択されたことを判別し、内部に記憶している最終取引ポイントと送信済みポイントとが一致するかどうかを判別する。図16に示すように、送信済みポイントはアドレス"2"を指し、最終取引ポイントはアドレス"5"を示しているとすると、IC部20は、送信済みポ

インタが指しているアドレス"2"の次のアドレス"3"から最終取引ポイントが指しているアドレス"5"までの取引履歴R3~R5を割り込み信号とカードID" C99"と個人公開鍵Pk2Aと共に電子マネー端末15Bに送信する(L31)。電子マネー端末15Bは、受信した取引履歴R3~R5とカードIDと個人公開鍵Pk2Aを電子マネーサーバ13へ送信する(L32)。

【0115】電子マネーサーバ13は、受信したカードID" C99"と個人公開鍵Pk2Aを確認要求と共に認証局11に送信する(L33)。認証局11は、自己が記憶するカードIDと個人公開鍵のリストに、受信したカードIDと個人公開鍵Pk2Aが登録されていることを確認し、確認完了電文を電子マネーサーバ13に送信する(L34)。

【0116】電子マネーサーバ13は、確認完了電文を受信すると、取引履歴R3~R5と自己が記憶している取引履歴とを突き合わせる。即ち、アドレス"3"~"5"の取引履歴R3~R5が全て電子マネーサーバ13に記憶されている取引履歴と一致することをチェックする。チェックの結果、取引履歴R3~R5が電子マネーサーバ13に記憶されている取引履歴と一致するならば、電子マネーサーバ13は、図2(A)に示す残高テーブルのカードID" C99"の残高を更新し、電子マネー端末15Bに突き合わせ完了電文を送信する(L35)。電子マネー端末15Bは、受信した突き合わせ完了電文を電子マネーカード19Aに送信する(L36)。電子マネーカード19Aは、突き合わせ完了電文を受信すると、図16に示すように、IC部20に記憶している送信済みポイントを"2"から"5"に更新する。

【0117】その後、電子マネー端末15と電子マネーカード19Aは指示されている電子マネーチャージ処理を実行する。

【0118】上述した突き合わせ処理では、電子マネーカード19からの取引履歴と電子マネーサーバ13に記憶されている電子マネー端末15からの取引履歴を比較する。これにより、不正に生成された(例えば、取引金額が改竄された)取引履歴を容易に検出することができる。また、不正が検出された際、不正な電子マネーカード19の光記憶部21に記憶されている取引履歴を参照することにより、いつ、どこで、いくら使用されたか、等の使用履歴を知ることができる。

【0119】(5) 電子マネー譲渡処理

次に、電子マネー譲渡処理の概要を図17を参照して説明する。電子マネーを譲渡(移転)する側を電子マネーカード19Aとし、譲渡を受ける側を電子マネーカード19Bとする。

【0120】図8(A)に示す画面表示に従って、表示部32に表示される処理メニューから「3) 電子マネー

の譲渡」が選択され、電子マネーカード19Aがカード挿入口35Aに電子マネーカード19Bがカード挿入口35Bにそれぞれ挿入され、電子マネーカード19Aから電子マネーカード19Bへの譲渡金額が入力される。電子マネー端末15は、この入力に回答して、電子マネーカード19Aと電子マネーカード19Bに、取引区分(19Aから19Bへの譲渡)と利用年月日と取引金額とから構成される取引情報と端末IDと、カードIDと個人公開鍵の要求を示す要求信号をそれぞれ送信する(P41)。

【0121】電子マネーカード19Aは、端末ID及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Aを用いて、端末IDと取引情報と自己のカードIDに対する取引認証子{Pk1A(端末ID+取引情報+19AのカードID)}を作成する。電子マネーカード19Aは、作成した取引認証子とカードIDと個人公開鍵Pk2Aとを電子マネー端末15に送信する(P42)。

【0122】また電子マネーカード19Bは、端末ID及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Bを用いて、端末IDと取引情報と自己のカードIDに対する取引先認証子{Pk1B(端末ID+取引情報+19BのカードID)}を作成する。電子マネーカード19Bは、作成した取引先認証子とカードIDと個人公開鍵Pk2Bとを電子マネー端末15に送信する(P42)。

【0123】電子マネー端末15は、電子マネーカード19Aから受信した取引認証子{Pk1A(端末ID+取引情報+19AのカードID)}とカードIDと個人公開鍵Pk2Aと、電子マネーカード19Bから受信した取引先認証子{Pk1B(端末ID+取引情報+19BのカードID)}とカードIDと個人公開鍵Pk2Bと、電子マネーカード19Aから電子マネーカード19Bに入力された金額(譲渡金額)を移動するよう指示する譲渡依頼電文とを、電子マネーサーバ13に送信する(P43)。なお、譲渡依頼電文は端末IDを含む。

【0124】電子マネーサーバ13は、受信した電子マネーカード19Aと電子マネーカード19BのカードID及び端末IDが事故カードIDリスト及び事故端末IDリストに登録されているかを判別する。

【0125】受信したカードID及び端末IDが、事故カードIDリスト及び事故端末IDリストに登録されていない場合、電子マネーサーバ13は、図2(A)に示す残高テーブルの電子マネーカード19Aの残高をチェックする。残高が不足している場合、残高不足の旨のメッセージを電子マネー端末15に送信する。電子マネー端末15は、残高不足のため、指示された金額が移転できない旨のメッセージを表示する。

【0126】残高が指示された譲渡金額以上の場合、電子マネーサーバ13は、電子マネーカード19Aの個人公開鍵Pk2Aを用いて取引認証子{Pk1A(端末ID+

取引情報+19AのカードID)}を端末IDと取引情報と電子マネーカード19AのカードIDとに変換する。又、電子マネーカード19Bの個人公開鍵Pk2Bを用いて取引先認証子{Pk1B(端末ID+取引情報+19BのカードID)}を端末IDと取引情報と電子マネーカード19BのカードIDとに変換する。次に、変換した内容が正しいかを判別する。即ち、取引認証子と取引先認証子から復号された取引情報及び端末IDが一致しており、取引認証子から変換されたカードIDが譲渡元の電子マネーカード19AのカードIDに一致し、取引先認証子から変換したカードIDが譲渡先の電子マネーカード19BのカードIDに一致することをチェックする。全て一致すると判別された場合、残高テーブルの電子マネーカード19Aと電子マネーカード19Bの残高をそれぞれ更新する。

【0127】次に、電子マネーサーバ13は、電子マネーカード19Aと電子マネーカード19BのカードID及び個人公開鍵を認証付与要求と共に認証局11に送信する(P44)。

【0128】認証局11は、認証付与要求に回答し、受信した電子マネーカード19Aと19BのカードID及び個人公開鍵Pk2A、Pk2Bを、自己が記憶するカードID及び個人公開鍵のリストに登録されているかをチェックする。これらが登録されていると判断された場合、それらに対してセンタ秘密鍵Ck1を用いて認証情報{Ck1(19AのカードID+Pk2A)}、{Ck1(19BのカードID+Pk2B)}をそれぞれ生成し、認証完了電文と共に電子マネーサーバ13に送信する(P45)。

【0129】電子マネーサーバ13は、認証完了電文に回答し、譲渡元の電子マネーカード19Aの取引履歴と譲渡先の電子マネーカード19Bの取引履歴を生成し記憶する。さらに、それらの取引履歴に認証局11からの認証情報を付加し、譲渡完了電文と共に電子マネー端末15に送信する(P46)。

【0130】電子マネー端末15は、取引履歴と認証情報を受信すると、センタ公開鍵Ck2を用いて認証情報をカードIDと個人公開鍵Pk2に変換し、チェックする。その認証情報が正しいものであると確認すると、譲渡完了電文に回答し、受信した取引履歴を電子マネーカード19Aと電子マネーカード19Bへそれぞれ送信する(P47)。電子マネーカード19Aと19BのIC部20は、受信した取引履歴に基づいて、それぞれが記憶している残高を更新する。即ち、電子マネーカード19AのIC部20は、受信した取引履歴に基づいて、記憶している残高を所定金額減額し、電子マネーカード19BのIC部20は、受信した取引履歴に基づいて、記憶している残高を所定金額増額する。

【0131】さらに、電子マネーカード19A、19BのIC部20は、それぞれ、最終取引ポイントの値を電

子マネー端末15に送信する。電子マネー端末15は、電子マネーカード19Aと19Bの光記憶部21の、最終取引ポイントの値が示すアドレスの次のアドレスに受信した取引履歴を追記する。さらに、最終取引ポイント及び送信済みポイントを、追記された取引履歴を示すように更新する。その後、電子マネー端末15は、電子マネーの譲渡が完了した旨を表示部32に表示すると共に電子マネーカード19Aと19Bを排出する。

【0132】この電子マネー譲渡処理を、利用者Aが電子マネーカード19A(カードID" C99")から電子マネーカード19B(カードID" C05")へ、電子マネー端末15C(端末ID" T150")を介して3万円分の電子マネーを譲渡する場合を例に図18を参照して説明する。

【0133】まず、利用者Aは、図8(A)に示す画面表示に従って、処理メニューから「3) 電子マネーの譲渡」を選択し、電子マネーカード19Aを譲渡元カード挿入口35Aに挿入し、電子マネーカード19Bを譲渡先カード挿入口35Bに挿入し、譲渡金額を入力する。

【0134】この入力に回答して、電子マネー端末15Cは、電子マネーカード19Aと電子マネーカード19Bに、取引区分と利用年月日と取引金額とから構成される取引情報と端末ID" T150"と共に、カードIDと個人公開鍵の要求を示す要求信号をそれぞれ送信する(L41)。

【0135】電子マネーカード19Aは、要求信号に回答し、端末ID" T150"と取引情報に自己のカードID" C99"を加え、個人秘密鍵Pk1Aを用いて取引認証子{Pk1A(T150+取引情報+C99)}を作成し、その取引認証子をカードID" C99"と個人公開鍵Pk2Aと共に電子マネー端末15Cに送信する(L42)。

【0136】また、電子マネーカード19Bは、要求信号に回答し、端末ID" T150"と取引情報に自己のカードID" C05"を加え、個人秘密鍵Pk1Bを用いて取引先認証子{Pk1B(T150+取引情報+C05)}を作成し、その取引先認証子をカードID" C05"と個人公開鍵Pk2Bと共に電子マネー端末15Cに送信する(L42)。

【0137】電子マネー端末15Cは、電子マネーカード19Aから受信したカードID" C99"と個人公開鍵Pk2Aと取引認証子{Pk1A(T150+取引情報+C99)}と、電子マネーカード19Bから受信したカードID" C05"と個人公開鍵Pk2Bと取引先認証子{Pk1B(T150+取引情報+C05)}と、電子マネーカード19Aから電子マネーカード19Bへ3万円の電子マネーを移動するよう指示する譲渡依頼電文とを、電子マネーサーバ13に送信する(L43)。なお、譲渡依頼電文は端末ID" T150"を含む。

【0138】電子マネーサーバ13は、受信した電子マ

ネーカード19Aと電子マネーカード19BのカードID" C99"、" C05"及び端末ID" T150"が事故カードID及び事故端末IDのリストに登録されているか否かをチェックする。カードID" C99"、" C05"及び端末ID" T150"が、事故カード又は事故端末として登録されていないと判別された場合、電子マネーサーバ13は、譲渡元の電子マネーカード19Aの残高を残高テーブルを参照してチェックする。

【0139】残高が3万円未満ならば、電子マネーサーバ13は、残高不足の旨のメッセージを電子マネー端末15に送信する。残高が3万円以上ならば、電子マネーサーバ13は、個人公開鍵Pk2Aを用いて取引認証子{Pk1A(T150+取引情報+C99)}を端末IDと取引情報と電子マネーカード19AのカードIDとに変換する。又、個人公開鍵Pk2Bを用いて取引先認証子{Pk1B(T150+取引情報+C05)}を端末IDと取引情報とカードIDとに変換する。

【0140】続いて、これらの内容が正しいか否かを判別する。即ち、取引認証子と取引先認証子から変換した端末IDと取引情報とが互いに一致しており、取引認証子から変換されたカードIDが譲渡元の電子マネーカード19AのカードID" C99"に一致し、取引先認証子から変換されたカードIDが譲渡先の電子マネーカード19BのカードID" C05"に一致するか否かをチェックする。チェックの結果、取引認証子と取引先認証子が正しいと判別されたならば、電子マネーサーバ13は、残高テーブルにおけるカードID" C99"の残高を3万円だけ減算し、カードID" C05"の残高に3万円を加算する。次に電子マネーサーバ13は、電子マネーカード19Aと電子マネーカード19BのカードID" C99"、" C05"及び個人公開鍵Pk2A、Pk2Bを認証局11に認証付与要求と共に送信する(L44)。

【0141】認証局11は、認証付与要求に回答し、自己が記憶するカードID及び公開鍵を参照することにより、受信した電子マネーカード19Aと電子マネーカード19BのカードID" C99"、" C05"及び個人公開鍵Pk2A、Pk2Bがこのシステムに登録されているか否かをチェックする。認証局11は、それらが登録されていることを確認すると、カードID" C99"、" C05"及び個人公開鍵Pk2A、Pk2Bに対してセンタ秘密鍵Ck1を用いて電子マネーカード19Aの認証情報{Ck1(C99+Pk2A)}と電子マネーカード19Bの認証情報{Ck1(C05+Pk2B)}をそれぞれ生成し、認証完了電文と共に電子マネーサーバ13に送信する(L45)。

【0142】電子マネーサーバ13は、電子マネーカード19Aと電子マネーカード19Bの認証情報{Ck1(C99+Pk2A)}と{Ck1(C05+Pk2B)}を受信すると、譲渡元の電子マネーカード19Aの取引履

歴と譲渡先の電子マネーカード19Bの取引履歴を生成し、取引履歴テーブルに記憶する。さらに、それらの取引履歴に認証局11からの認証情報を付与し、譲渡完了電文と共に電子マネー端末15Cに送信する(L46)。

【0143】電子マネー端末15は、取引履歴と認証情報を受信すると、センター公開鍵Ck2を用いて認証情報をカードIDと個人公開鍵Pk2に変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴を電子マネーカード19Aと19BのIC部20にそれぞれ送信する(L47)。電子マネーカード19Aと19BのIC部20は、受信した取引履歴に基づいて記憶回路に記憶している残高を更新する。即ち、電子マネーカード19Aは残高を3万円減額し、電子マネーカード19Bは残高を3万円増額する。さらに、電子マネー端末15Cは、電子マネーカード19Aと19BのIC部20から最終取引ポイントの値を読み出し、電子マネーカード19Aと19Bの光記憶部21の最終取引ポイントの値が示すアドレスの次のアドレスに、取引履歴をそれぞれ追記する。

【0144】さらに、電子マネー端末15Cは、電子マネーカード19Aと19BのIC部20に記憶されている最終取引ポイント及び送信済みポイントを追記された取引履歴を示すように更新する。その後、電子マネー端末15Cは、電子マネーの譲渡が完了した旨を表示部32に表示すると共に電子マネーカード19Aと19Bを排出する。

【0145】なお、譲渡元の電子マネーカード19Aの残高のチェックは、「3）電子マネーの譲渡」がメニューより選択され、譲渡金額が入力されたときに電子マネー端末15が行うようにしてもよい。この場合、電子マネー端末15は、電子マネーカード19Aに残高要求を行う。

【0146】また、電子マネーカード19Aが挿入された電子マネー端末15Cと電子マネーカード19Bが挿入された電子マネー端末15Dとの間で電子マネーが譲渡されるような構成にしてもよい。2台の電子マネー端末15C、15D間での譲渡処理について図19を参照して以下説明する。この説明では、電子マネーを譲渡(移転)する側を電子マネー端末15Cとし、譲渡を受ける側を電子マネー端末15Dとする。

【0147】まず、電子マネーカード19Aが電子マネー端末15Cに、電子マネーカード19Bが電子マネー端末15Dにそれぞれ挿入され、譲渡元の電子マネー端末15Cに、電子マネーの譲渡指示と、譲渡先の電子マネー端末15Dを特定する情報(例えば、端末ID)が入力される。電子マネー端末15Cは、この入力にตอบสนองして、電子マネーカード19Aに、カードIDと個人公開鍵の要求を示す要求信号と取引情報と端末IDとを送信する(L61)と共に、電子マネーサーバ13へ譲渡

先の電子マネー端末15Dを特定する特定情報を送信する(L62)。

【0148】電子マネーサーバ13は、電子マネー端末15Cから特定情報を受信すると、その特定情報が示す電子マネー端末15Dに、その端末が譲渡先として指定されたこと通知する通知信号を送信する(L63)。電子マネー端末15Dは、電子マネーサーバ13からの通知信号にตอบสนองして、電子マネーカード19Bに、カードIDと個人公開鍵の要求を示す要求信号と取引情報と端末IDとを送信する。(L64)

【0149】電子マネー端末15Cに挿入された電子マネーカード19Aは、端末ID及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Aを用いて、端末IDと取引情報と自己のカードIDに対する取引認証子{Pk1A(端末ID+取引情報+19AのカードID)}を作成する。電子マネーカード19Aは、作成した取引認証子とカードIDと個人公開鍵Pk2Aとを電子マネー端末15Cに送信する(L65)。

【0150】また電子マネー端末15Dに挿入された電子マネーカード19Bは、端末ID及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Bを用いて、端末IDと取引情報と自己のカードIDに対する取引先認証子{Pk1B(端末ID+取引情報+19BのカードID)}を作成する。電子マネーカード19Bは、作成した取引先認証子とカードIDと個人公開鍵Pk2Bとを電子マネー端末15Dに送信する(L66)。

【0151】電子マネー端末15Cは、電子マネーカード19Aから受信した取引認証子{Pk1A(端末ID+取引情報+19AのカードID)}とカードIDと個人公開鍵Pk2Aと譲渡依頼電文とを、電子マネーサーバ13に送信する。(L67) また、電子マネー端末15Dは、電子マネーカード19Bから受信した取引先認証子{Pk1B(端末ID+取引情報+19BのカードID)}とカードIDと個人公開鍵Pk2Bと、自己が譲渡元であることを示す譲渡元電文を、電子マネーサーバ13に送信する(L68)。なお、譲渡依頼電文と譲渡元電文は端末IDを含む。

【0152】電子マネーサーバ13は、受信した電子マネーカード19A、19BのカードID及び電子マネー端末15C、15Dの端末IDが事故カードIDリスト及び事故端末IDリストに登録されているか否かを判別する。

【0153】受信したカードID及び端末IDが、事故カードIDリスト及び事故端末IDリストに登録されていない場合、電子マネーサーバ13は、図2(A)に示す残高テーブルの電子マネーカード19Aの残高をチェックする。残高が不足している場合、残高不足の旨のメッセージを電子マネー端末15Cに送信する。電子マネー端末15Cは、残高不足のため、指示された金額が移転できない旨のメッセージを表示する。

【0154】残高が指示された譲渡金額以上の場合、電子マネーサーバ13は、電子マネーカード19Aの個人公開鍵Pk2Aを用いて取引認証子{Pk1A(端末ID+取引情報+19AのカードID)}を端末IDと取引情報と電子マネーカード19AのカードIDとに変換する。又、電子マネーカード19Bの個人公開鍵Pk2Bを用いて取引先認証子{Pk1B(端末ID+取引情報+19BのカードID)}を端末IDと取引情報と電子マネーカード19BのカードIDとに変換する。次に、変換した内容を照合してそれらが正しいか否かを判別する。それらの内容が正しいと判別された場合、残高テーブルの電子マネーカード19Aと電子マネーカード19Bの残高をそれぞれ更新する。

【0155】次に、電子マネーサーバ13は、電子マネーカード19Aと電子マネーカード19BのカードID及び個人公開鍵を認証付与要求と共に認証局11に送信する(L69)。

【0156】認証局11は、認証付与要求に回答し、受信した電子マネーカード19A、19BのカードID及び個人公開鍵Pk2A、Pk2Bを、自己が記憶するカードID及び個人公開鍵のリストに登録されているか否かをチェックする。これらが登録されていると判断された場合、それらに対してセンタ秘密鍵Ck1を用いて認証情報{Ck1(19AのカードID+Pk2A)}、{Ck1(19BのカードID+Pk2B)}をそれぞれ生成し、認証完了電文と共に電子マネーサーバ13に送信する(L70)。

【0157】電子マネーサーバ13は、認証完了電文に回答し、譲渡元の電子マネーカード19Aの取引履歴と譲渡先の電子マネーカード19Bの取引履歴を生成し記憶する。さらに、それらの取引履歴に認証局11からの認証情報を付加し、譲渡完了電文と共に電子マネー端末15Cと電子マネー端末15Dにそれぞれ送信する(L71)。

【0158】電子マネー端末15Cと電子マネー端末15Dは、取引履歴と認証情報をそれぞれ受信すると、センタ公開鍵Ck2を用いて認証情報をカードIDと個人公開鍵Pk2に変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴をそれぞれの電子マネーカード19A、19Bへ送信する(L72)。電子マネーカード19Aと19BのIC部20は、受信した取引履歴に基づいて、それぞれが記憶している残高を更新する。即ち、電子マネーカード19AのIC部20は、受信した取引履歴に基づいて、記憶している残高を所定金額減額し、電子マネーカード19BのIC部20は、受信した取引履歴に基づいて、記憶している残高を所定金額増額する。

【0159】さらに、電子マネーカード19A、19BのIC部20は、最終取引ポイントの値を電子マネー端末15C、15Dにそれぞれ送信する。電子マネー端末

15C、15Dは、それぞれの電子マネーカード19A、19Bの光記憶部21の、最終取引ポイントの値が示すアドレスの次のアドレスに受信した取引履歴を追記する。さらに、最終取引ポイント及び送信済みポイントを、追記された取引履歴を示すように更新する。その後、電子マネー端末15C、15Dは、電子マネーの譲渡が完了した旨を表示すると共にそれぞれの電子マネーカード19A、19Bを排出する。

【0160】以上の説明では、電子マネーの譲渡処理をオンライン処理により実行したが、譲渡額が一定額以下の場合には、電子マネー支払処理と同様、電子マネー端末15内で処理するオフライン方式にしてもよい。これにより、レスポンス速度を向上することができる。オフライン処理の場合、セキュリティを高めるため、1回の譲渡金額の限度を定めてもよい。

【0161】(6) 電子マネー換金処理

次に、電子マネーカード19に蓄積している電子マネーを換金し、利用者の決済口座に振り込む電子マネー換金処理の概要を図20を参照して説明する。まず、利用者は、図8に示すように、表示部32に表示される処理メニューから「2) 電子マネーの換金」を選択し、電子マネーカード19を電子マネー端末15に挿入し、換金金額を入力する。

【0162】電子マネー端末15は、この選択に回答し、取引区分と利用年月日と取引金額とから構成される取引情報と端末IDと、カードIDと個人公開鍵の要求を示す要求信号とを、電子マネーカード19に送信する(P51)。

【0163】電子マネーカード19は、要求信号に回答し、端末IDと取引情報に自己のカードIDを加え、個人秘密鍵Pk1を用いて取引認証子{Pk1(端末ID+取引情報+カードID)}を作成し、作成した取引認証子をカードIDと個人公開鍵と共に電子マネー端末15に送信する(P52)。

【0164】電子マネー端末15は、受信したカードIDに取引情報と端末IDを加え、端末秘密鍵Tk1を用いて取引先認証子{Tk1(端末ID+取引情報+カードID)}を作成する。電子マネー端末15は、作成した取引先認証子{Tk1(端末ID+取引情報+カードID)}と、入力された換金金額と、電子マネーカード19から対応する決済口座に振り替えることを指示し、端末公開鍵Tk2を含む換金要求と、電子マネーカード19のカードIDと、個人公開鍵Pk2とを電子マネーサーバ13に送信する(P53)。なお、換金要求は、送信元の電子マネー端末15の端末IDを含む。

【0165】電子マネーサーバ13は、受信した電子マネーカード19のカードID及び端末IDを自己が記憶する事故カードIDリスト及び事故端末IDのリストに登録されているか否かをチェックする。受信したカードID及び端末IDが、事故カードIDリスト及び事故端

末IDリストに登録されていないと判別された場合、電子マネーサーバ13は、受信した個人公開鍵Pk2を用いて取引認証子{Pk1(端末ID+取引情報+カードID)}を端末IDと取引情報とカードIDとに変換する。又、受信した端末公開鍵Tk2を用いて取引先認証子{Tk1(端末ID+取引情報+カードID)}を端末IDと取引情報とカードIDとに変換し、これらが一致するか否かを判別する。これらが一致した場合、電子マネーサーバ13は、取引認証子{Pk1(端末ID+取引情報+カードID)}と取引先認証子{Tk1(端末ID+取引情報+カードID)}は正しいと判別し、カードID及び個人公開鍵Pk2を認証付与要求と共に認証局11に送信する(P54)。

【0166】認証局11は、認証付与要求に应答し、自己が記憶しているカードID及び個人公開鍵のリストを参照することにより、受信したカードIDと個人公開鍵Pk2がシステムに登録されているかをチェックする。それらが登録されているならば、認証局11は、センタ秘密鍵Ck1を用いて、受信したカードID及び個人公開鍵Pk2に対する認証情報{Ck1(カードID+Pk2)}を生成し、電子マネーサーバ13に送信する(P55)。受信したカードID及び個人公開鍵Pk2がシステムに登録されていないならば、認証局11は不正検出を電子マネーサーバ13に通知する。

【0167】電子マネーサーバ13は、認証局11から認証情報{Ck1(カードID+Pk2)}を受信すると、残高テーブルを参照して電子マネーカード19Aの残高をチェックし、振替可能であれば、カードIDと振替金額を含む振替依頼電文を作成し、銀行センタ17に送信する(P56)。

【0168】なお、受信したカードIDと端末IDの少なくとも一方が使用不可のカードID及び端末IDのリストのいずれかと一致する場合、又は取引認証子と取引先認証子から変換された端末IDと取引情報とカードIDとが互いに一致しない場合、電子マネーサーバ13は、電子マネー端末15にチャージ不可の旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。また、電子マネーカード19の残高が不足している場合は、電子マネーサーバ13は、残高不足の旨のメッセージを電子マネー端末15に送信する。

【0169】銀行センタ17は、振替依頼電文を受信すると、図5に示す口座テーブルを参照して、指示された金額を別段口座からカードIDに対応する決済口座に振り替える(P57)。振り替え完了後、銀行センタ17は、振替完了電文を電子マネーサーバ13に送信する(P58)。

【0170】電子マネーサーバ13は、振替完了電文を受信すると、電子マネーカード19の残高テーブルの残高を更新し、取引履歴を生成し、取引履歴テーブルに記

憶する。次に電子マネーサーバ13は、認証局11からの認証情報{Ck1(カードID+Pk2)}を取引履歴に付与し、換金が完了したことを示す換金完了電文と共に電子マネー端末15に送信する(P59)。

【0171】電子マネー端末15は、取引履歴と認証情報{Ck1(カードID+Pk2)}と振替完了電文とを受信すると、センタ公開鍵Ck2を用いて認証情報{Ck1(カードID+Pk2)}をカードIDと個人公開鍵Pk2に変換し、チェックする。その認証情報が正しいものであると確認すると、電子マネーカード19に取引履歴を送信する(P60)。

【0172】電子マネーカード19のIC部20は、受信した取引履歴に基づいて、残高を更新すると共に最終取引ポイントの値を電子マネー端末15に送信する。電子マネー端末15は、受信した取引履歴を光記憶部21の最終取引ポイントが指示するアドレスの次のアドレスに追記する。続いて、IC部20に記憶されている最終取引ポイントと送信済みポイントを更新する。その後、電子マネー端末15は、電子マネーの換金が完了した旨を表示部32に表示すると共に電子マネーカード19を排出する。

【0173】この電子マネー換金処理を、利用者Aが電子マネーカード19A(カードID" C99")に記憶している電子マネーのうち5万円を、電子マネー端末15B(端末ID" T150")を用いて、銀行センタ17の自己の決済口座に振り替える場合を例に図21を参照して説明する。利用者Aは、表示部32に表示される処理メニューから「2)電子マネーの換金」を選択し、電子マネーカード19Aを電子マネー端末15Bに装着し、換金金額「5万円」を入力部33に入力する。

【0174】この操作に应答して、電子マネー端末15Bは、電子マネーカード19Aに、取引区分と利用年月日と取引金額とから構成される取引情報と、端末ID" T150"と、カードIDと個人公開鍵の送信を要求する要求信号と、を送信する(L51)。電子マネーカード19Aは、要求信号に应答し、受信した端末ID" T150"及び取引情報に自己のカードID" C99"を加え、個人秘密鍵Pk1Aを用いて取引認証子{Pk1A(T150+取引情報+C99)}を作成する。電子マネーカード19Aは、作成した取引認証子{Pk1A(T150+取引情報+C99)}とカードID" C99"と個人公開鍵Pk2Aを電子マネー端末15Bに送信する(L52)。

【0175】電子マネー端末15Bは、受信したカードID" C99"に取引情報と端末ID" T150"を加え、端末秘密鍵Tk1を用いて取引先認証子{Tk1B(T150+取引情報+C99)}を作成する。電子マネー端末15Bは、作成した取引先認証子{Tk1B(T150+取引情報+C99)}と、入力された換金金額を電子マネーカード19Aからその電子マネーカード1

9Aに対応する決済口座に振り替えることを指示し、端末公開鍵Tk2Bを含む換金要求と、電子マネーカード19AのカードID" C99"と、個人公開鍵Pk2Aと、取引認証子{Pk1A(T150"+取引情報+C99)}とを電子マネーサーバ13へ送信する(L53)。

【0176】電子マネーサーバ13は、電子マネーカード19AのカードID" C99"及び端末ID" T150"が事故カードIDリスト及び事故端末IDリストに登録されているか否かをチェックする。受信したカードID" C99"及び端末ID" T150"が、事故カードIDリスト及び事故端末IDリストに登録されていないと判別された場合、電子マネーサーバ13は、受信した個人公開鍵Pk2Aを用いて取引認証子{Pk1A(T150"+取引情報+C99)}を取引情報とカードIDと端末IDに変換する。さらに、受信した端末公開鍵Tk2Bを用いて取引先認証子{Tk1B(T150"+取引情報+C99)}を取引情報とカードIDと端末IDに変換し、これらが相互に一致するか否かを判別する。完全に一致した場合、電子マネーサーバ13は、カードID" C99"と個人公開鍵Pk2Aを認証付与要求と共に認証局11に送信する(L54)。

【0177】認証局11は、自己が記憶しているカードID及び個人公開鍵を参照し、受信したカードID" C99"と個人公開鍵Pk2Aがシステムに登録されているかをチェックし、登録済みであることを確認すると、センタ公開鍵Ck1を用いて認証情報{Ck1(C99+Pk2A)}を生成し、認証完了電文と共に電子マネーサーバ13に送信する(L55)。電子マネーサーバ13は、認証局11から認証完了電文と認証情報{Ck1(C99+Pk2A)}を受信すると、残高テーブルのカードID" C99"の残高が換金金額の5万円以上か否かを判別する。残高が5万円以上ならば、電子マネーサーバ13は、銀行センタ17へカードID" C99"と振替金額"5万円"を含む振替依頼電文を送信する(L56)。

【0178】銀行センタ17は、電子マネーサーバ13から振替依頼電文を受信すると、口座テーブルを参照し、別段口座からカードID" C99"に対応する利用者Aの決済口座に5万円を振り替える。振替処理が完了すると、銀行センタ17は振替完了電文を電子マネーサーバ13に送信する(L57)。電子マネーサーバ13は、振替完了電文を受信すると、残高テーブルのカードID" C99"の残高から5万円を減算し、取引履歴を生成し、取引履歴テーブルに記憶する。次に、電子マネーサーバ13は、認証局11からの認証情報{Ck1(C99+Pk2A)}を取引履歴に付与し、換金完了電文と共に電子マネー端末15Bに送信する(L58)。

【0179】電子マネー端末15Bは、換金完了電文に
40 応答し、センタ公開鍵Ck2を用いて認証情報{Ck1

(C99+Pk2A)}をカードC99と個人公開鍵Pk2に変換し、チェックする。その認証情報が正しいものであると確認すると、取引履歴を電子マネーカード19Aに送信する(L59)。電子マネーカード19AのIC部20は、受信した取引履歴に基づいて、自己が記憶する残高から5万円を減算する。さらに、電子マネー端末15Bは、受信した取引履歴を光記憶部21の最終取引ポイントが指示する位置に追記し、最終取引ポイント及び送信済みポイントの値を更新する。その後、電子マネー端末15Bは、電子マネーの換金が完了した旨を表示部32に表示すると共に電子マネーカード19Aを排出する。

【0180】このようにして、利用者は自己の電子マネーカード19に蓄積している電子マネーを換金し、自己の決済口座に振り込むことができる。

【0181】なお、電子マネー端末15が電子マネーカード19の残高のチェックを行うようにしてもよい。この場合、電子マネー端末15は、電子マネーカード19に残高を要求する信号を送信する。

【0182】以上説明したように、この電子マネーシステムにより、電子マネーを電子マネーカードにチャージし、換金し、譲渡し、支払いに使用することができる。しかも、光記憶部21に取引履歴を記録するので、この追記型記憶部の記録内容を検証(追尾)することにより、不正行為等を容易に検出することができる。さらに、センタにおいても取引履歴を記録することにより、不正行為をより確実に検出することができる。

【0183】なお、この発明は上記実施の形態に限定されず、種々の変形及び応用が可能である。例えば、取引履歴の構成要素は任意であり、各取引に一意な取引ID、その時点での電子マネーの残高、取引時分秒等を取引履歴に含めても良い。また、認証情報等を取引履歴から削除してもよい。

【0184】光記憶部21に記録する取引履歴からそのカードを特定する情報を省略してもよい。例えば、ある電子マネーカード19に電子マネーをチャージした場合、その電子マネーカード19の光記憶部21には、例えば、取引がチャージであること、取引日時、取引金額、端末ID等を記録し、自己を特定する情報は記録する必要がない。

【0185】同様に、例えば、電子マネーカード19Aから電子マネーカード19Bに電子マネーを移動した場合に、電子マネーカード19Aの光記憶部21には、取引区分が電子マネーの譲渡であること、譲渡先の電子マネーカード19BのカードID、移転金額等を記録し、移転元(電子マネーカード19A)を特定する情報を記録せず、電子マネーカード19Bの光記憶部21には、電子マネーの譲受であること、譲渡元の電子マネーカード19AのカードID、移転金額等を記録し、移転先
50 (電子マネーカード19B)を特定する情報を記録しな

いように構成してもよい。これにより、光記憶部21の記録データの量を削減できる。

【0186】上記実施の形態では、電子マネーカードの利用者の決済口座のリストを銀行センタ17に登録し、カードIDを決済口座の口座番号に変換したが、決済口座の口座番号を電子マネーカード19のIC部20又は光記憶部21に登録しておき、電子マネーのチャージ、換金等の処理を行う際に、電子マネーカード19から口座番号を銀行センタ17に通知してもよい。

【0187】上記実施の形態では、個人認証情報に含まれる署名を生成、確認するために署名鍵Skと検査鍵Ekを用いたが、センタ秘密鍵Ck1とセンタ公開鍵Ck2を用いてもよい。

【0188】また、電子マネーの譲渡として、店舗における支払いを処理することも可能である。この場合、顧客の電子マネーカード19から店舗の電子マネーカード19へ売上げ金額相当の電子マネーを譲渡するという処理の形態をとる。例えば、図4(B)に示す電子マネー端末15は、顧客の電子マネーカード19Aを挿入するためのカード挿入口35の他に、端末所有者側(店舗、販売員、販売管理者等を含む)の電子マネーカード19Bを挿入するためのカード挿入口を備えることとする。店舗用カード挿入口には、開店時等に、端末所有者側の電子マネーカード19Bを挿入しておく。

【0189】売上計算が終了すると、電子マネー端末15(例えばPOS端末)は表示部32に売り上げ金額と支払い方法を問い合わせるメッセージを表示する。このメッセージに応じて、電子マネーによる支払いを選択し、顧客の電子マネーカード19Aを挿入口に挿入する。以後の処理は、上述の譲渡処理と同一である。

【0190】なお、上述のオフラインでの譲渡処理を採用してもよい。

【0191】また、上記説明では、IC部20は、光記憶部21に記憶される取引履歴のうち、最後の取引履歴の位置を記憶するようにしているが、IC部20が記憶する位置は、新たに取引履歴を書き込む際に有用な位置情報であればよく、任意である。例えば、IC部20は、最後の取引履歴の次の位置を記憶するようにしてもよい。

【0192】なお、各取引において、残高が不足した場合は取引不可としていたが、残高不足のメッセージを電子マネー端末15に表示し、利用者取引金額を再入力させるようにしてもよい。

【0193】ワイドエリアのネットワーク(例えば、インターネット等)のネットワーク上でこの電子マネーシステムを構築する場合は、認証局11と電子マネーサーバ13をそれぞれ設けることが望ましいが、クローズドループ型のローカルネットワークでは、認証局11と電子マネーサーバ13を、1つのサーバとして実現してもよい。

【0194】また、この電子マネーシステムを、図22に示すように、認証局11を除いた構成にしてもよい。この場合の、各処理の概要を図23～図27に示す。この場合の処理は、図23～図27と従前の図面を参照すれば明かなように、センタ秘密鍵及びセンタ公開鍵、個人秘密鍵及び個人公開鍵、認証に関する処理がなくなった点を除けば、実施の形態の動作と同一である。この構成によれば、システム全体において処理速度が向上する。また、認証局11を除いた場合、電子マネー端末15が入力された取引指示に基づいて取引履歴を生成し、電子マネーカードに書き込むと共に電子マネーサーバ13にその取引に関する情報を送信するようにしてもよい。電子マネーサーバ13は、受信した情報を基に取引履歴テーブルにその取引の取引履歴を記憶する。

【0195】なお、上述した個人認証情報発行処理において電子マネーカード19の個人公開鍵は既に登録されているため、電子マネーカード19の取引認証子を送信する際、個人公開鍵を送信しなくても良い。同様に、電子マネー端末15の端末公開鍵をセンタ10に登録しておけば、電子マネー端末15の取引先認証子を送信する際、端末公開鍵を送信しなくても良い。

【0196】認証局11に電子マネーカード19のカードIDと個人公開鍵Pk2を送信し、認証局11がそれらに対して署名することにより生成される認証情報の代わりに、電子マネーカード19発行時等に予めカード内に記憶させている個人認証子を用いてもよい。また、認証局11による認証情報生成の対象として、例えば、換金金額、日付等の取引情報等を用いてもよい。この場合、電子マネーサーバ13は取引履歴と認証情報Ck1(取引情報)を電子マネー端末15に送信し、電子マネー端末15はセンタ公開鍵Ck2を用いて受信した認証情報を確認する。これにより、その取引がなされたことをより確実に確認することができる。

【0197】認証局11は、認証付与要求に応じて、Ck1(カードID+個人公開鍵Pk2+”取引許可の電文”)を認証情報として生成しても良い。”取引許可の電文”は、チャージ処理の場合は”チャージ許可の電文”とする等、取引の種別に応じた許可電文としてもよい。また、認証情報としてCk1(”取引許可の電文”)を用いても良い。また、この”取引許可の電文”中に、電子マネーサーバ13が生成した乱数を含めるようにしてもよい。これにより、偽造が極めて困難となる。

【0198】また、システムのセキュリティを高めるため、例えば、電子マネー端末15の操作者の正当性を操作者の身体的特徴に基づいて判別してもよい。例えば、電子マネーカード19のIC部20の記憶回路に所持者の指紋データを配置しておき、電子マネー端末15の操作者の指紋をスキャンし、これらが一致する場合にのみ、以後の電子マネー取引処理を実行してもよい。

【0199】この場合、電子マネー端末15には、図2

8に示すような指紋読取装置41が接続される。指紋読取装置41は、指紋をスキャンするための読取窓41Aと指を案内するためのガイド41Bを備える。また、IC部20の記憶回路には、保持者の指紋の画像をフーリエ変換した後、抽出された位相情報が予め登録されている。

【0200】指紋読取装置41は、図29に示すように、読取窓41A内の画像（指紋の画像）をスキャンし、画像データを取得する画像取得部51と、画像取得部51で取得した画像データ（の波形）をフーリエ変換するフーリエ変換部52と、フーリエ変換部52で取得されたフーリエ級数の位相情報のみを抽出する位相情報抽出部53と、IC部20から読み出した位相情報と位相情報抽出部53で生成された位相情報を合成する位相合成部54と、合成部54で合成された位相情報をフーリエ変換して相関強度を得るフーリエ変換部55と、フーリエ変換部55で得られた相関強度と閾値を比較し、操作者が正当者であるか否かを判別する判別部56とより構成される。

【0201】このような構成において、例えば、処理メニューの中から処理を選択し、電子マネーカード19を挿入すると、電子マネー端末15は、図30に示すように、指紋読取装置41上に指を置くべき旨のメッセージを表示部32に表示する。操作者がメッセージに従って指紋読取装置41上に指を置くと、指紋読取装置41の画像取得部51は、読取窓41A内の指紋をスキャンし、その画像を取り込む。フーリエ変換部52は、読み取られた画像をフーリエ変換し、位相情報抽出部53が位相情報を取り込む。

【0202】続いて、位相合成部54は、IC部20に登録されている位相情報を読み出し、位相情報抽出部53から抽出された位相情報と合成し、さらに、フーリエ変換部55は合成データをフーリエ変換し、相関強度を求める。

【0203】判定部56は、相関強度が一定値以上の場合に、予めIC部20に登録されている指紋と読み取った指紋が類似し、操作者が電子マネーカード19の正当な保持者であると判別し、選択した処理に対応する以後の処理を可能とするように制御する。相関強度が一定値未満の場合、予めIC部20に登録されている指紋と読み取った指紋が類似しないと判断し、表示部32に指紋照合が一致しないため、以後の操作ができない旨を表示し、電子マネーカード19を排出する。

【0204】このような構成によれば、操作者の身体的特徴に基づいて、操作者が正当な者か否かを判別し、電子マネーの取引を許可するか否かを判別することができる。従って、電子マネーの不正使用を有効に防止できる。

【0205】なお、指紋の類似度を判別する手法及び回路は図28に示す回路及び方法に限定されず、他の手法

を使用してもよい。また、身体的特徴としては、指紋に限らず、声紋、顔のパターン、網膜パターン等を使用してもよい。声紋を使用する場合には、声紋の特徴データをIC部20に格納し、電子マネー端末15にマイクロフォンを配置し、マイクロフォンで取得した音声の特徴データを抽出し、IC部20に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別する。

【0206】また、顔のパターン、網膜パターン等を使用する場合には、顔、網膜パターンの特徴データをIC部20に格納し、電子マネー端末15にカメラを配置し、カメラで取得した、画像の特徴データを抽出し、IC部20に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別する。

【0207】なお、予め抽出された特徴データは、IC部20に格納されてもよく、光記憶部21に格納されても良い。また、取引の際に使用した身体的特徴を示す特徴データを光記憶部21に取引履歴情報の一部として記録してもよい。

【0208】電子マネーを扱うシステムでは、例えば、利用者のカードID等の情報を入手して、そのカードIDの所有者になりすまして認証を得ようとする不正行為が考えられる。このような不正行為を防ぐために、通信電文等を例えばRSA方式等の暗号方式を用いて暗号化することにより、そのセキュリティを高めることができる。

【0209】この場合、例えば、認証局11は、センタ秘密鍵Ck1とセンタ公開鍵Ck2を生成し、記憶する。認証局11は、電子マネーサーバ13にセンタ秘密鍵Ck1をコピーすることにより、センタ秘密鍵Ck1をセンタ10内で共有化する。また、認証局11は、センタ公開鍵Ck2を各電子マネー端末15及び電子マネーカード19等に電子マネーサーバ13を介して予め配布する。

【0210】各電子マネーカード19及び電子マネー端末15は、センタ公開鍵Ck2を用いて各々の情報（電子マネーカード19ならばカードID及び個人公開鍵、電子マネー端末15ならばチャージ要求、種々の電文等）を暗号化し、電子マネーサーバ13に送信する。電子マネーサーバ13がセンタ秘密鍵Ck1を用いてそれらの情報を復号化し、処理する。電子マネーサーバ13は、電子マネーカード19から送られてきた個人公開鍵を用いて取引履歴を暗号化し、電子マネー端末15を介して電子マネーカード19に送信する。

【0211】このような手法を用いることにより、電子マネーカード19及び電子マネー端末15からの情報は、センタ10内の電子マネーサーバ13及び認証局11しか復号化することができず、又、電子マネーサーバ13からの取引履歴は、電子マネー端末15で参照されことなく、電子マネーカード19に送信され、復号化

される。更に、秘密鍵・公開鍵を定期的に変更することにより、よりセキュリティを高めることができる。

【0212】なお、認証局11は、センタ秘密鍵Ck1及びセンタ公開鍵Ck2を定期的又は不定期に変更し、センタ公開鍵Ck2を電子マネー端末15へ、センタ秘密鍵Ck1を電子マネーサーバ13へ、それぞれ送信する。センタ秘密鍵Ck1及びセンタ公開鍵Ck2を変更した後、電子マネー端末15に電子マネーカード19が挿入されたとき、電子マネー端末15は、新たなセンタ公開鍵Ck2を電子マネーカード19に通知する。

【0213】また、暗号化の方式は、公開鍵方式に限定されず、共通鍵方式を用いてもよい。この場合、セキュリティの面から電子マネーカード19の耐タンパー性を強化することが望ましい。

【0214】また、このシステムで取引が行われる度に、新たな暗号化のキー（秘密鍵と公開鍵の対、共通鍵等）を発行し、電子マネーカードに通知して、通知されたキーを用いて暗号化・復号化を行ってもよい。

【0215】さらに、キーを乱数に基づいて発生してもよい。このようなシステムによれば、次に発行されるキーの予測がつかず、情報の漏洩を防止できる。過去に発行されたキーと新たに発行されたキーを組み合わせる暗号化及び復号化用のキーとして使用してもよい。例えば、今回のキー K_t と前回のキー K_{t-1} を組み合わせる $\{K_t + K_{t-1}\}$ をキーとして用いて各種情報を暗号化し、さらに、復号化してもよい。

【0216】電子マネーシステムにおいては、電子マネーカード19自体の完全なコピーを作成し、不正使用することが考えられる。この種の不正使用を防止するためには、電子マネーサーバ13で、取引毎に固有の番号を電子マネーカード19に付与し、オンライン取引開始時に、電子マネーカード19からこの固有番号を電子マネーサーバ13に送信し、電子マネーサーバに登録されているその電子マネーカード19の固有番号に一致することを確認してから取引を行い、取引終了時等に、新たな固有番号を発生して電子マネーカード19と電子マネーサーバ13に登録するように構成すればよい。この構成によれば、取引の度に、固有番号が更新されるため、電子マネーカード19のコピーを作成しても、1回取引を行うと、使用した1枚以外は固有番号が電子マネーサーバ13に登録されているものと異なってしまうため、使用できなくなる。従って、電子マネーカード19のコピーによる不正使用を防止できる。

【0217】

【発明の効果】以上説明したように、本発明によれば、電子マネーカードに格納されている電子マネーを換金することができる。しかも、追記型記憶部に取引履歴を記録するので、この追記型記憶部の記録内容を検証することにより、不正行為等を容易に検出することができる。さらに、センタにおいても取引履歴を記録することによ

り、不正行為をより確実に検出することができる。また、電子マネーを取引する際に、操作者の身体的特徴に基づいてその正当性を判別することにより、取引の信頼性を高めることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図2】(A)は、電子マネーサーバが記憶している残高テーブルの構造を示す図、(B)は、電子マネーサーバが記憶している事故カードリストの構造を示す図、

(C)は、電子マネーサーバが記憶している事故端末リストの構造を示す図である。

【図3】電子マネーサーバが記憶している取引履歴テーブルの構造を示す図である。

【図4】(A)と(B)は、電子マネー端末の外観構成の例を示す図である。

【図5】銀行センタが記憶している口座テーブルの構造を示す図である。

【図6】電子マネーカードの構造を示す図である。

【図7】電子マネーチャージ処理の概要を示す図である。

【図8】(A)～(C)は、電子マネー端末の表示例を示す図である。

【図9】電子マネーチャージ処理の流れを説明するための図である。

【図10】個人認証情報発行処理の概要を示す図である。

【図11】個人認証情報発行処理の流れを説明するための図である。

【図12】電子マネー支払い処理の概要を示す図である。

【図13】電子マネー支払い処理の流れを説明するための図である。

【図14】突き合わせ処理の概要を示す図である。

【図15】突き合わせ処理の流れを説明するための図である。

【図16】突き合わせ処理において未送信履歴の送信前と送信後のIC部と光記憶部と残高テーブルの状態を示す図である。

【図17】電子マネー譲渡処理の概要を示す図である。

【図18】電子マネー譲渡処理の流れを説明するための図である。

【図19】2台の電子マネー端末間での電子マネー譲渡処理の流れを説明するための図である。

【図20】電子マネー換金処理の概要を示す図である。

【図21】電子マネー換金処理の流れを説明するための図である。

【図22】認証局を含まない場合の電子マネーシステムの構成の一例を示す図である。

【図23】認証局を含まない場合の電子マネーチャージ

処理の流れを示す図である。

【図24】認証局を含まない場合の電子マネー支払い処理の流れを示す図である。

【図25】認証局を含まない場合の突き合わせ処理の流れを示す図である。

【図26】認証局を含まない場合の電子マネー譲渡処理の流れを示す図である。

【図27】認証局を含まない場合の電子マネー換金処理の流れを示す図である。

【図28】指紋読取装置の例を示す図である。

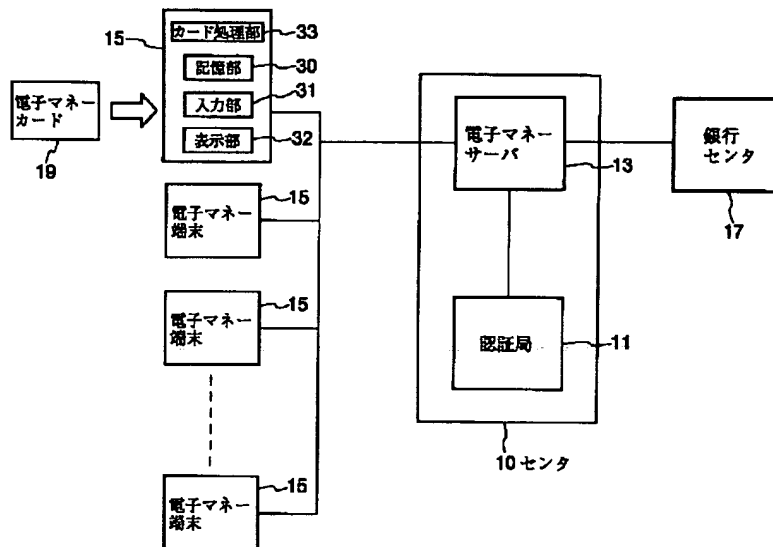
【図29】指紋照合回路の構成例を示す図である。

【図30】指紋照合時の電子マネー端末の表示例を示す図である。

【符号の説明】

- 10 センタ
- 11 認証局
- 13 電子マネーサーバ
- 15 電子マネー端末
- 19 電子マネーカード
- 20 IC部
- 21 光記憶部
- 30 記憶部
- 31 入力部
- 32 表示部
- 33 カード処理部
- 34 タッチパネル
- 35、35A、35B カード挿入口
- 36 金銭ドロア

【図1】



【図3】

取引履歴テーブル

カードID: CXXX

利用区分	利用年月日	取引金額	端末ID	取引先のカードID 又は端末ID	取引先	
					取引先ID	取引先名
チャージ	1998/02/20	30000	T111	T111	XXXXXXXX	XXXXXXXX
譲渡	1998/04/15	50000	T128	C099	XXXXXXXX	XXXXXXXX
支払	1998/05/18	45000	T288	T288	XXXXXXXX	XXXXXXXX
換金	1998/09/25	10000	T451	T451	XXXXXXXX	XXXXXXXX
.
.
.
.

取引情報

【図2】

(A) 残高テーブル

カードID	残高
C001	50000
C003	10000
C005	5000
C018	30000
⋮	⋮
⋮	⋮
⋮	⋮

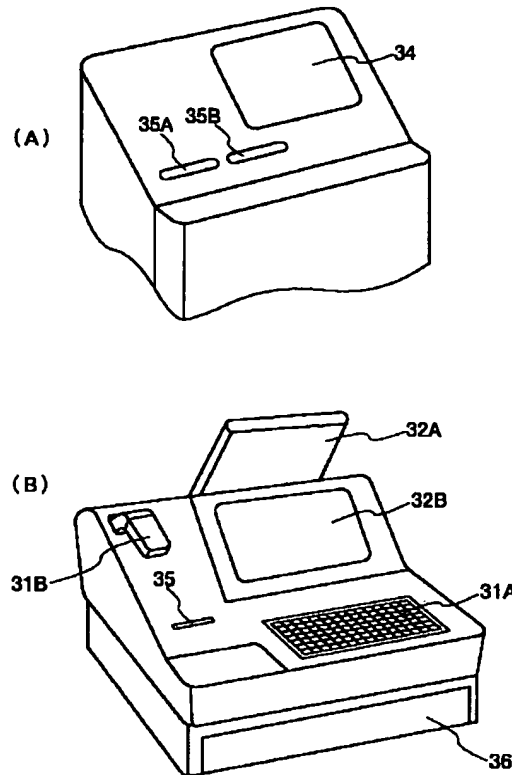
(B) 事故カードリスト
(使用不可の電子マネーカード
のカードIDリスト)

カードID (使用不可)
C010
C021
C033
C048
⋮
⋮
⋮

(C) 事故端末リスト
(使用不可の電子マネー端末
の端末IDのリスト)

端末ID
T145
T247
T255
T301
⋮
⋮
⋮

【図4】

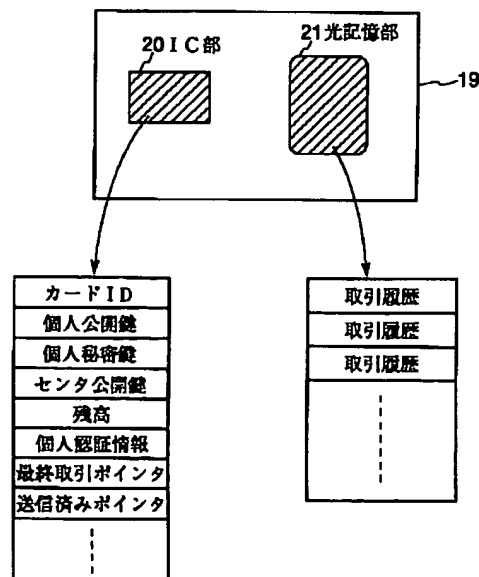


【図5】

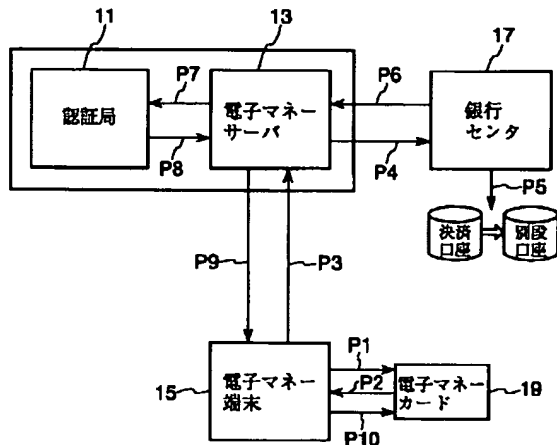
口座テーブル

カードID	口座番号
C01	10002221
C03	12341234
C05	53334442
⋮	⋮
⋮	⋮
C89	30000001
⋮	⋮
⋮	⋮

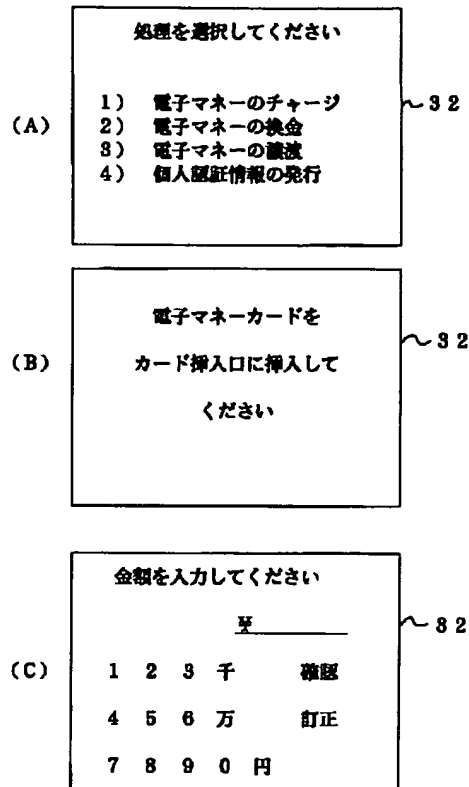
【図6】



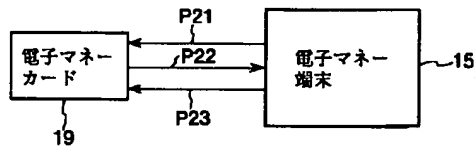
【図7】



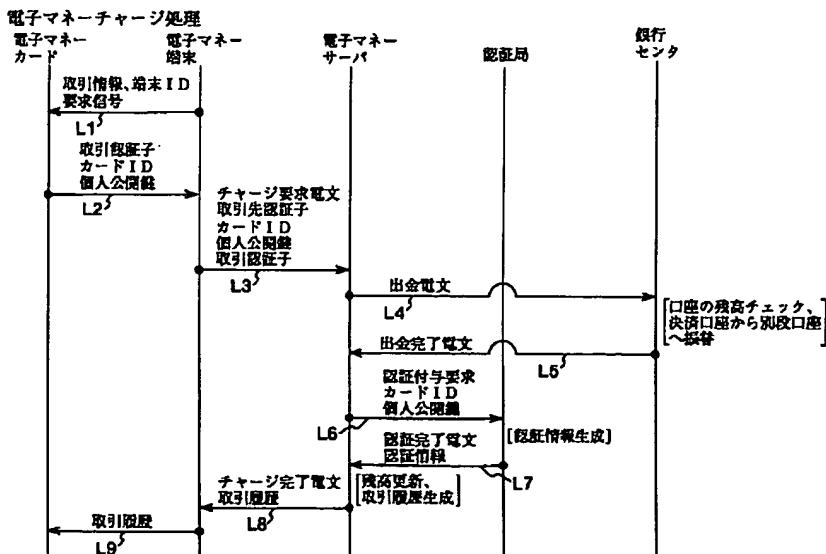
【図8】



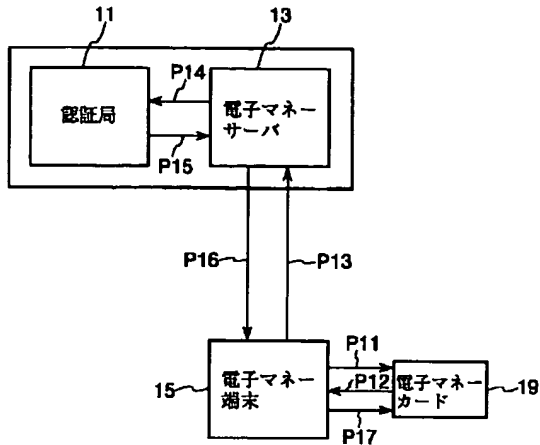
【図12】



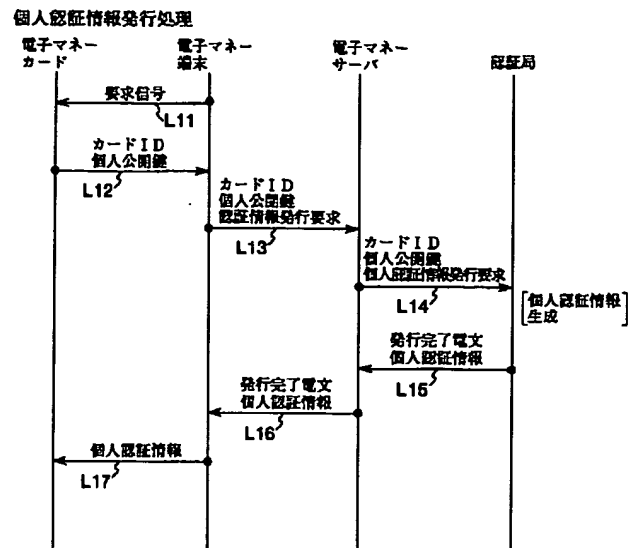
【図9】



【図10】

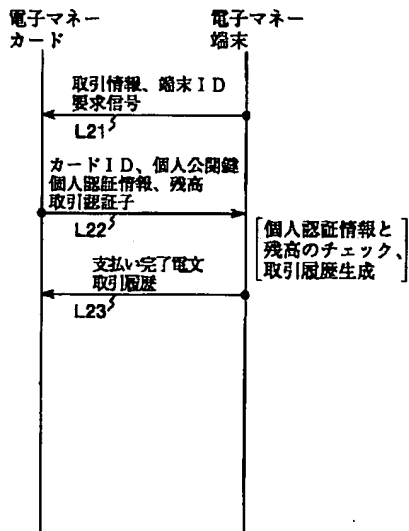


【図11】

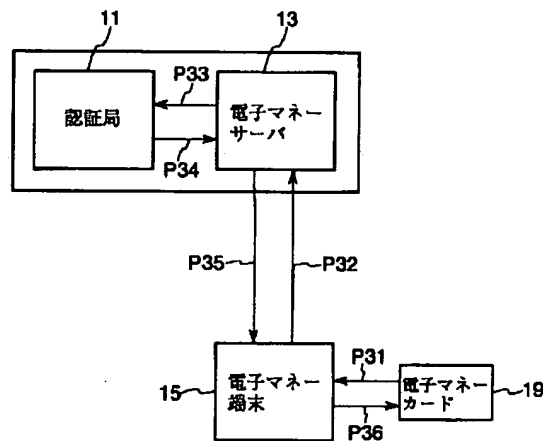


【図13】

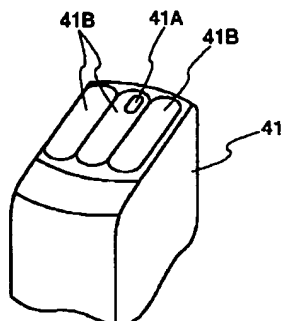
電子マネー支払い処理



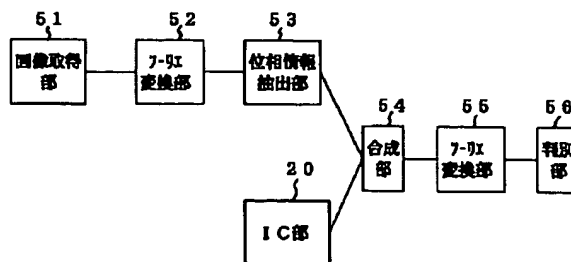
【図14】



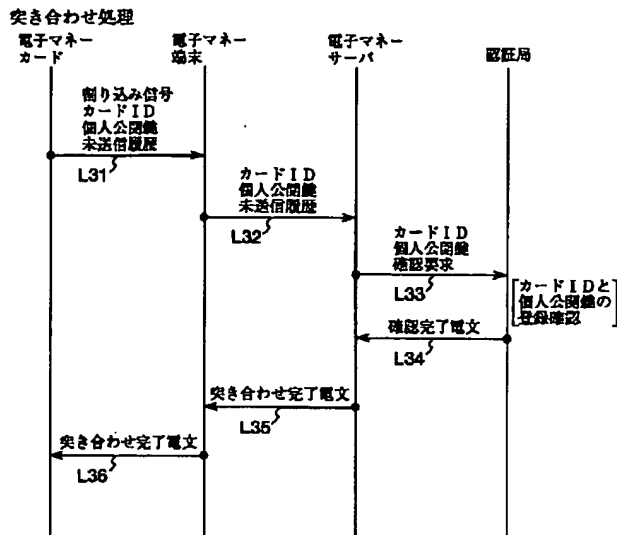
【図28】



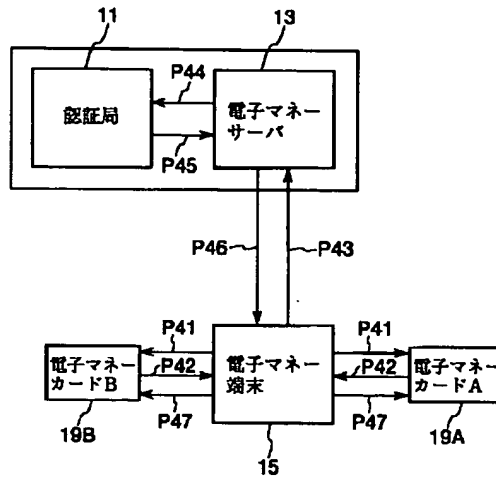
【図29】



【図15】

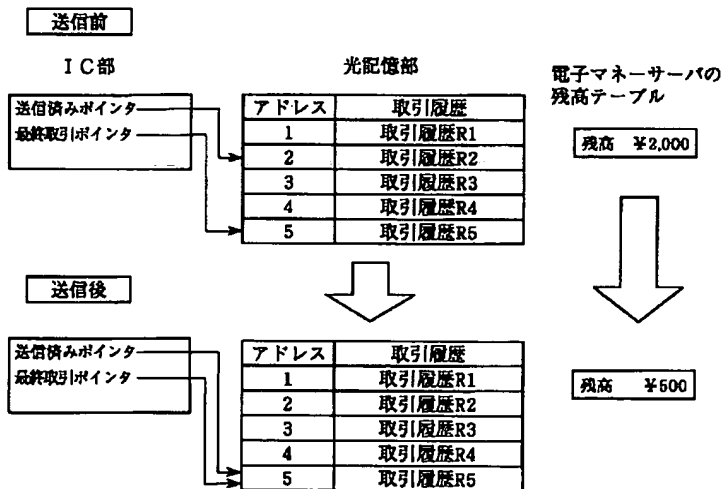


【図17】

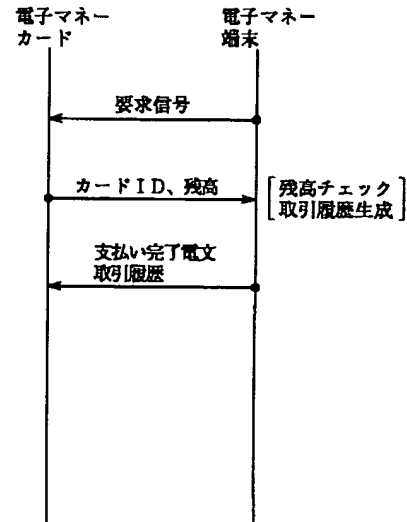


【図24】

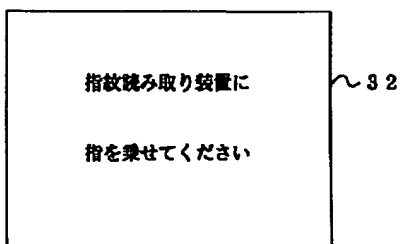
【図16】



電子マネー支払い処理（認証局を設置しない場合）

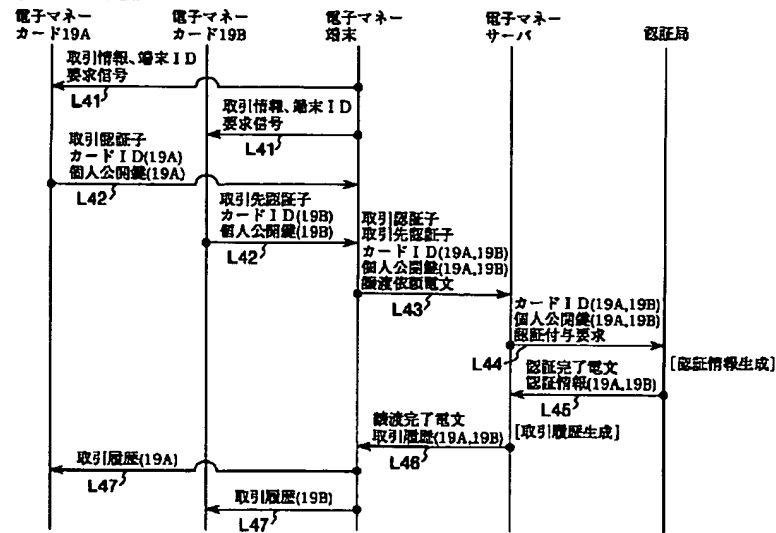


【図30】



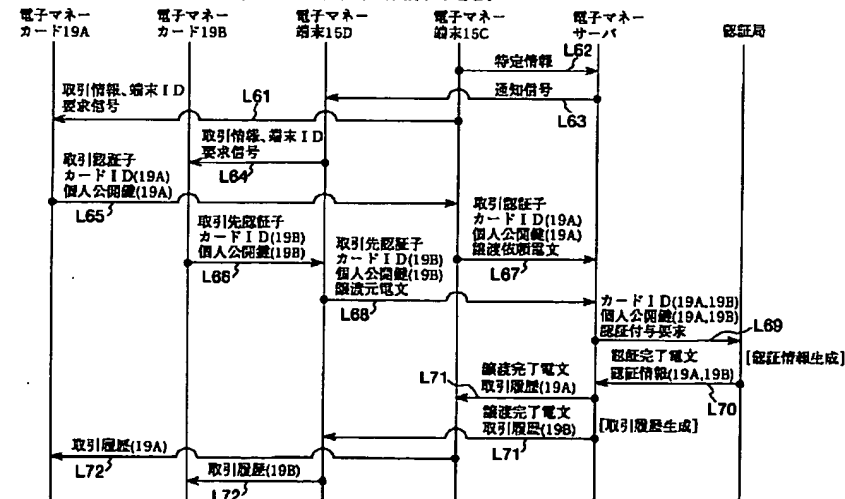
【図18】

電子マネー譲渡処理

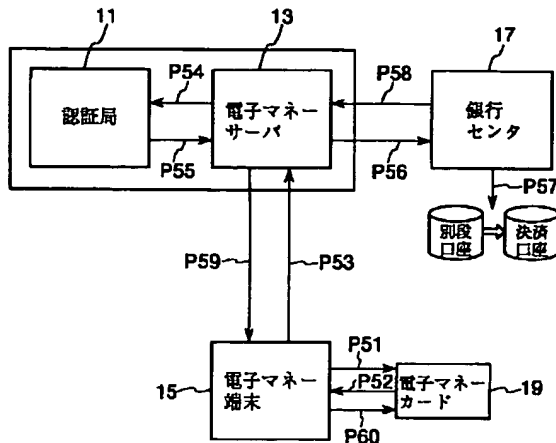


【図19】

電子マネー譲渡処理 (2台の電子マネー端末間で譲渡する場合)

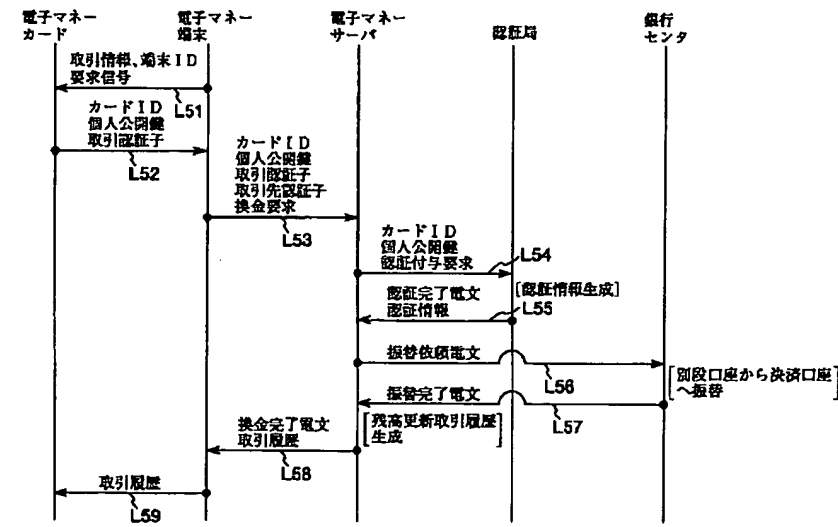


【図20】

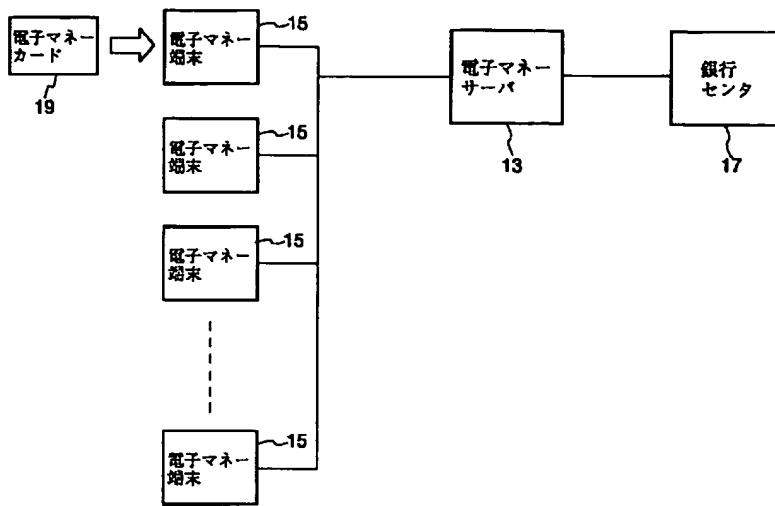


【図21】

電子マネー換金処理

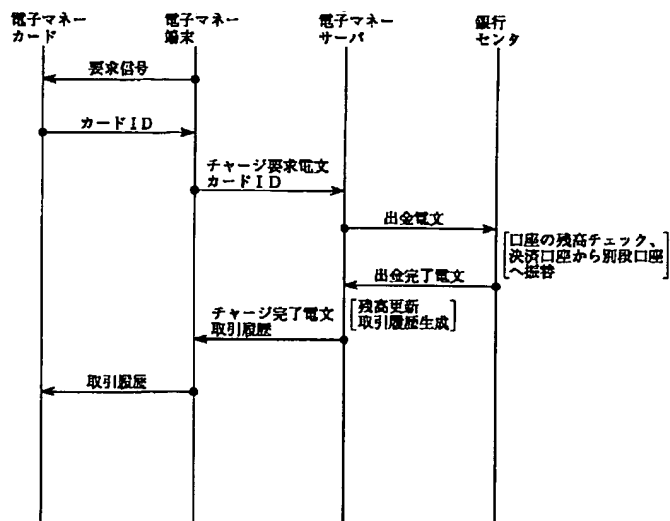


【図22】



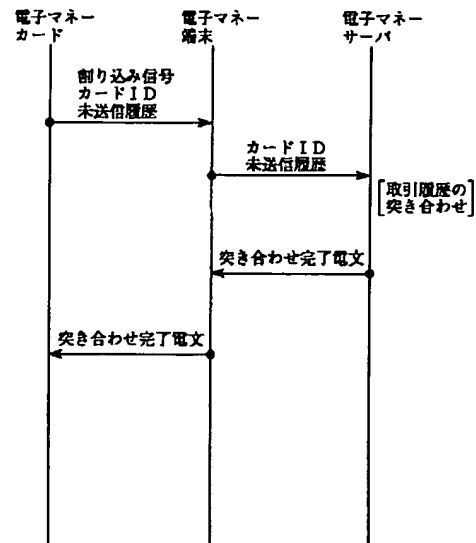
【図23】

電子マネーチャージ処理（認証局を設けない場合）



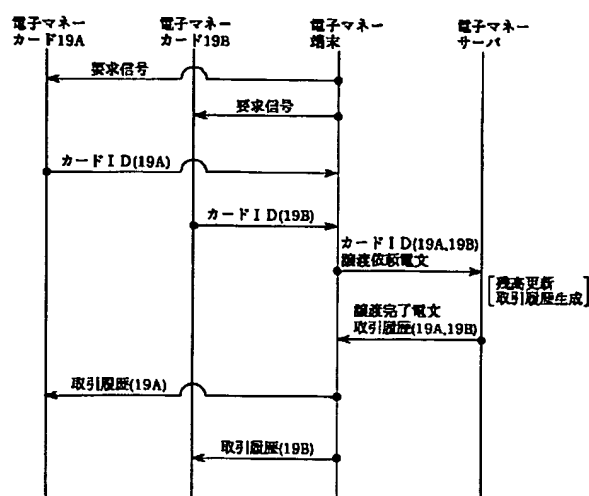
【図25】

突き合わせ処理（認証局を設けない場合）



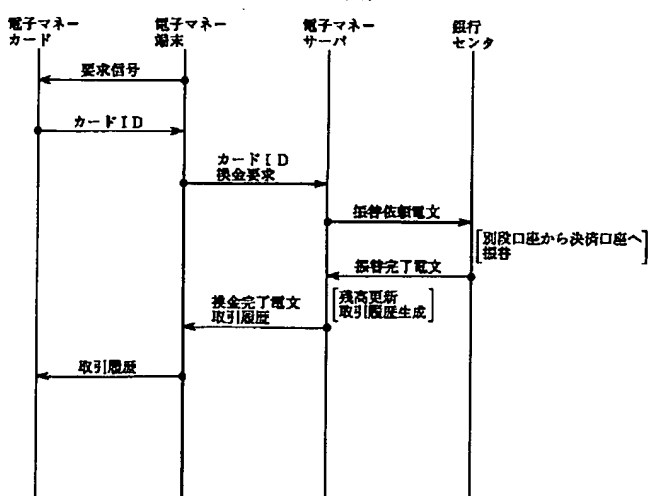
【図26】

電子マネー譲渡処理（認証局を設置しない場合）



【図27】

電子マネー換金処理（認証局を設置しない場合）



フロントページの続き

(72)発明者 新開 伊知郎
東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72)発明者 北田 豊浩
東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.